IMPLEMENTACIÓN DE SERVIDOR SIP
(SESSION INITIATION PROTOCOL)

ANDRES BOTERO PATIÑO
ANDRES PARRA LONDOÑO

Tesis de Grado para optar al titulo de Ingeniero Electrónico

Director:
IVÁN HERRERA MURGUEITIO
Ingeniero Electrónico
Profesor Programa de Ingeniería Electrónica

Asesor externo:
JUAN GUILLERMO CASTAÑEDA DELGADO
Ingeniero Electricista

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERIA
DEPARTAMENTO DE ENERGÉTICA Y ELECTRÓNICA
INGENIERÍA ELECTRÓNICA
SANTIAGO DE CALI
2004

Nota de aceptación:

Trabajo aprobado por el comité de grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Occidente para optar al título de Ingeniero Electrónico

ZEIDA MARÍA ZOLARTE
_____
Jurado

ALEXANDER GARCÍA
_____
Jurado

Santiago de Cali, 30 junio del 2004

A nuestras familias por su apoyo incondicional en este proceso de aprendizaje que se ve finalizado con los mejores frutos y grandes expectativas para un futuro exitoso.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Juan Guillermo Castañeda, Ingeniero Electricista, Gerente General de IPSOFACTUM LTDA, por sus valiosos aportes en infraestructura, equipos, conocimiento y apoyo. También le agradecemos por el entusiasmo que siempre mostró hacia el desarrollo y crecimiento de la tecnología que se expone en este proyecto.

Iván Herrera Murgueitio, Ingeniero Electrónico, Profesor del Programa de Ingeniería Electrónica de la Universidad Autónoma de Occidente, por sus orientaciones permanentes y ayuda en la conceptualización de temas referentes a este proyecto.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

GLOSARIO

ADPCM (ADAPTATIVE DIFFERENCIAL PCM). Método digital de transmisión de datos análogos mediante algoritmos que detectan la diferencia de información en el tiempo, para disminuir la cantidad de información modulada mediante pulsos codificados.

ADSL (ASYMETRIC DIGITAL SUBSCRIBER LINE). Método de transmisión de datos a través de las líneas telefónicas tradicionales manejando un canal distinto al de voz con un ancho de banda superior.

ANCHO DE BANDA. El ancho de banda es la máxima cantidad de datos que pueden pasar por un canal de comunicaciones en un momento dado.

ASCII (AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE). Código de 7-bit que sustituye las letras del alfabeto romano por cifras y otros caracteres informáticos.

ATA (ANALOG TELEPHONE ADAPTER). Adaptador de Teléfono Análogo. Es un dispositivo electrónico cuya función es convertir las señales producidas por un teléfono análogo convencional a señales digitales compatibles con el protocolo de enlace Ethernet y con el protocolo de red IP.

ATM (ASYNCHRONOUS TRANSFER MODE). Modo de Transferencia Asíncrona. Estándar que define la conmutación de paquetes de tamaño fijo con alta carga, alta velocidad y asignación dinámica de ancho de banda.

B2BUAWM (BACK TO BACK USER AGENT WITH MEDIA). Este elemento tramita todo el tráfico de multimedia y mensajes SIP desde adentro hacia afuera de una red privada.

BACKBONE. Enlace de gran caudal o serie de nodos que forman un eje de conexión principal. Es la infraestructura que necesaria para soportar una red de área amplia.

BASE DE DATOS. Una base de datos es un formato estructurado para organizar y mantener información que puede ser fácilmente recuperada.

BINDING. Ligamento o enlace entre direcciones y/o puertos IP y máquinas dentro de una red.

BPS (BITS PER SECOND). Bits por segundo, una medida de la velocidad a la cual son transmitidos los datos.

BYTE. Es una serie de 8 bits.

CABLE MODEM. Dispositivo que permite tener acceso a datos a muy alta velocidad mediante una conexión CATV.

CCITT (CONSULTATIVE COMMITTEE FOR INTERNATIONAL TELEGRAPH AND TELEPHONE). Comité Consultivo Internacional de Telefonía y Telegrafía.

CGI (COMMON GATEWAY INTERFACE). Programa de interfaz que permite al servidor de Internet ejecutar programas externos para realizar una función específica.

CODEC. Algoritmo software usado para comprimir/ descomprimir señales de voz, audio y video.

CRIPTOGRAFÍA. Es el arte de enmascarar información con signos normales que solo tienen sentido a la luz de una clave secreta.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL). Protocolo de Configuración Dinámica del equipo.

DIFFSERV (DIFFERENTIATED SERVICES INTERNET QOS MODEL). Modelo de Calidad de Servicio en Internet basado en Servicios Diferenciados.

DIRECCIÓN IP. Código numérico que es asignado a un ordenador o equipo específico en el Internet.

DIRECCIÓN MAC. Dirección que identifica un dispositivo de red específico. Dirección física.

DMZ (DESMILITARIZED ZONE). Zona desmilitarizada. Se refiere a una conexión sin restricciones o protecciones de tipo lógico.

DNS (DOMAIN NAME SYSTEM). Sistema de Nombres de Dominio.

DTMF (DUAL TONE MULTI FUNCTION). Función Múltiple por Tono Dual, es una adaptación del sistema de llamada de telefonía digital actualmente en uso en los teléfonos de teclas, consiste en la transmisión simultánea de dos tonos audibles y de frecuencias no relacionadas armónicamente.

ENCRIPTACIÓN. Ver Criptografía.

ETHEREAL. Software gratuito para análisis de redes.

ETHERNET. Protocolo de Nivel de Enlace.

EXTRANET. Red que permite a una empresa compartir información contenida en su Intranet con otras empresas y con sus clientes.

FCP (FIREWALL CONTROL PROTOCOL). Protocolo de Control de Firewall.

FQDN (FULLY QUALIFIED DOMAIN NAME). Nombre de Dominio Enteramente Calificado.

FIREWALL. Es el método o dispositivo para proteger una red, separándola lógicamente de otra red en la cual no se confía.

FTP (FILE TRANSFER PROTOCOL). Protocolo de transporte de Ficheros. Método muy común para transferir uno o más ficheros de un ordenador a otro.

GATEKEEPER. Es la unidad central de control que gestiona las prestaciones en una red de Voz o Fax sobre IP, o de aplicaciones multimedia y de videoconferencia.

GATEWAY. Pasarela entre dos redes.

H.323. Recomendación global de la Unión Internacional de Telecomunicaciones (ITU) que fija los estándares para las comunicaciones multimedia sobre redes basadas en paquetes que no proporcionan una Calidad de Servicio (QoS, Quality of Service) garantizada.

HANDSHAKE. Protocolo que permite al emisor y receptor ponerse de acuerdo a la hora de intercambiar datos entre ellos. Permite negociar la velocidad de transferencia inicial y variarla a medida que transcurre el intercambio de datos.

HOST. Es un ordenador directamente conectado a una red que efectúa las funciones de un servidor y alberga servicios.

HTML (HYPERTEXT MARKUP LANGUAGE). Lenguaje informático utilizado para crear documentos de hipertexto.

HTTP (HYPERTEXT TRANSFER PROTOCOL). Protocolo de transporte de Hipertexto.

ICMP (INTERNET CONTROL MESSAGES PROTOCOL). Protocolo de Mensajes de Control de Internet.

IETF (INTERNET ENGINEERING TASK FORCE). Grupo de Trabajo de Ingeniería de Internet.

IGMP (INTERNET GROUP MANAGEMENT PROTOCOL). Protocolo de Gestión de Grupos en Internet.

IM&P (INSTANT MESSAGING). Mensajería Instantánea. Sistema de intercambio de mensajes escritos en tiempo real a través de la Red.

INTERNET-DRAFT. Documento no oficial o borrador que se pone a disposición pública para recibir todas las recomendaciones y correcciones antes de ser un RFC.

INTRANET. Internet interno diseñado para ser utilizado dentro de una empresa, universidad u organización.

INTSERV (INTEGRATED SERVICES INTERNET QOS MODEL). Modelo de Calidad de Servicio en Servicios Integrados de Internet.

IP (INTERNET PROTOCOL). Protocolo de Internet.

IP MULTICAST. Extensión del Protocolo Internet para dar soporte a comunicaciones de multidifusión.

IP TELEPHONY. Tecnología para la transmisión de llamadas telefónicas ordinarias sobre Internet u otras redes de paquetes utilizando PC`s, gateways y teléfonos estándar.

IP UNICAST (UNIDIFUSIÓN). Comunicación establecida entre un solo emisor y un solo receptor en una red.

IPv4. Es la versión 4 del Protocolo de Internet. Las direcciones IP referentes a esta versión poseen un tamaño de 32 bits.

IPv6. Es la versión 6 del Protocolo de Internet. Las direcciones IP referentes a esta versión poseen un tamaño de 128 bits.

IPBX (INTERNET PROTOCOL PRIVATE BRANCH EXCHANGE). Central Privada basada en IP.

ISDN (INTEGRATED SERVICES DIGITAL NETWORK). RDSI, (Red Digital de Servicios Integrados).

ISP (INTERNET SERVICE PROVIDER). Proveedor de Servicios Internet, PSI.

ITU-T (INTERNATIONAL TELECOMMUNICATIONS UNION – TELECOMMUNICATIONS). Unión Internacional de Telecomunicaciones – Telecomunicaciones.

JITTER (VARIACIÓN DE RETARDO). Se refiere al nivel de variación de retado en la entrega de datos que introduce una red.

LAN (LOCAL AREA NETWORK). Red de Área Local, se refiere a la red local que conecta ordenadores situados en el mismo piso, en el mismo edificio o en edificios cercanos.

LINUX. Sistema operativo de Open Source (Libre Distribución) basado en el sistema operativo UNIX.

LOGIN NAME. Es el identificador del usuario requerido al acceder a un sistema.

LPC (LINEAR PREDICTIVE CODING). Codificación lineal predictiva.

MASCARA DE SUBRED. Mecanismo para dividir una red en varias subredes para darle características de privacidad y administración a la red total.

MBONE (MULTICAST BACKBONE). Red Troncal de Multidifusión.

MEGACO (MEDIA GATEWAY CONTROL). Control de Pasarela de Medios.

MEMORIA CACHÉ. Espacio de memoria en el cual se almacena temporalmente información que es utilizada continuamente.

MGCP (MEDIA GATEWAY CONTROL PROTOCOL). Protocolo de Control de Pasarela de Medios.

MIME (MULTIPURPOSE INTERNET MAIL EXTENSION). Sistema que permite integrar dentro de un mensaje de correo electrónico ficheros binarios.

MODEM (MODULATOR DEMODULATOR). Dispositivo electrónico encargado de convertir las señales digitales a análogas y viceversa.

MULTIMEDIA. Utilización simultánea de más de un tipo de medio.

MULTIPLEXACIÓN. Método por el cual mediante un algoritmo, implementado en hardware o software, se puede transmitir algún tipo de información especifica por un mismo canal compartido.

MYSQL. Gestor gratuito de Bases de datos de buena capacidad de almacenamiento de información y manejo de comandos de consulta SQL.

NAT (NETWORK ADDRESS TRANSLATOR). Traductor de Direcciones de Red de Trabajo.

OUTSOURCING. Se refiere a subcontratación de servicios por parte de una Empresa.

PASARELA. Ver Gateway.

PACKET SWITCHING (CONMUTACIÓN DE PAQUETES). Técnica de conmutación en la cual los mensajes se dividen en paquetes antes de su envío.

PBX (PRIVATE BRANCH EXCHANGE). Central Telefónica Privada.

PCM (PULSE CODE MODULATION). Método digital de transmisión de datos análogos mediante la modulación de pulsos codificados.

PLUG-IN. Es un módulo opcional que puede ser agregado a una aplicación específica.

PPP (POINT-TO-POINT PROTOCOL). Protocolo Punto a Punto. Es un protocolo de comunicaciones utilizado para empaquetar y transmitir/recibir datos a través de las líneas análogas.

PROXY. Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada.

PSTN (PUBLIC SWITCHED TELEPHONE NETWORK). Red de Telefonía Pública Conmutada.

QOS (QUALITY OF SERVICE). Calidad de Servicio.

RAS (REGISTRATION, AUTHENTICATION AND STATUS). Registro, Autentificación y Estado.

RFC (REQUEST FOR COMMENTS). Serie de documentos que describen el conjunto de protocolos de Internet y experimentos similares.

RJ11. Conector de cable de línea telefónica (4 hilos).

RJ45. Conector de Cable de Red de Datos (8 hilos).

ROUTER. Enrutador. Dispositivo hardware o software que distribuye tráfico entre redes.

RTCP (REAL TIME CONTROL PROTOCOL). Protocolo de Control de Transporte en Tiempo-real.

RTP (REAL TIME PROTOCOL). Protocolo de Transporte en Tiempo-real.

SAP (SESSION ANNUNCIATION PROTOCOL). Protocolo de Anuncio de Sesión.

SCN (SWITCHED CIRCUIT NETWORK). Red de Circuitos Conmutados.

SDP (SESSION DESCRIPTION PROTOCOL). Protocolo de Descripción de Sesión.

SIP (SESSION INITIATION PROTOCOL). Protocolo de Inicio de Sesión.

SIP ALG. Software que le permite re-escribir paquetes SIP a un Firewall.

SIP URI. Es el formato utilizado por el SIP para identificar a los usuarios.

SMTP (SIMPLE MAIL TRANSFER PROTOCOL). Protocolo de transferencia de correo electrónico.

SOFTPHONE. Aplicación de Software diseñada para trabajar con protocolos que manejan VoIP como SIP y H.323.

SQL (SENTENCE QUERY LENGUAJE). Es un Lenguaje de sentencias de pregunta que permite establecer consultas en bases de datos locales o remotas.

SS7 (SIGNALLING SYSTEM NUMBER 7). Sistemas de Señales número 7.

STUN (SIMPLE TRAVERSAL OF UDP TROUGH NAT). Cruce Simple de Paquetes UDP a través de un NAT.

TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL). Protocolo de Control de Transporte / Protocolo de Internet.

TDM (TIME DIVISION MULTIPLEXING). Multiplexado por División de Tiempo.

TELNET. Programa que permite acceder a ordenadores distantes en Internet a los cuales se tiene permiso de acceso.

TLS (TRANSPORT LAYER SECURITY). Seguridad de la capa de transporte.

TURN (TRAVERSAL USING RELAY NAT). Cruce Usando NAT de Relevo.

UTF-8 Es un mecanismo estándar usado por Unicode para codificar valores de caracteres amplios en una secuencia de bytes.

UDP (USER DATAGRAM PROTOCOL). Protocolo de Datagramas de Usuario. Es un protocolo de transporte que se utiliza para enviar paquetes de información en enlaces no orientados a conexión.

UNIX. Sistema operativo interactivo y de tiempo compartido de enorme popularidad en los ambientes académicos y empresariales.

VLAN (VIRTUAL LOCAL AREA NETWORK). Red de Área Local Virtual.

VOIP (VOICE OVER IP). Voz sobre IP. Método de envío de voz por redes IP.

WAN (WIDE AREA NETWORK). Red que conecta equipos geográficamente alejados.

WEBMASTER. Persona encargada del mantenimiento y administración de un sitio web.

XDSL. Cualquiera de las tecnologías de Líneas de Suscripción Digital.

RESUMEN

En este documento se plantea toda la teoría necesaria para el entendimiento del protocolo SIP y absolutamente todos los procesos y protocolos que permiten una comunicación de voz sobre IP entre dos usuarios, cualquiera sea su ubicación. Además, se da una guía completa para implementar un servicio de telefonía en Internet, siguiendo todos los pasos para que se logre un mejoramiento continuo y una evolución de esta teoría, siendo esta el futuro de la telefonía multiusuario.

En este documento se exponen también las soluciones prácticas a las limitantes y conflictos que se presentan en distintos escenarios de uso de los servicios de voz sobre IP para lograr la implementación correcta de estos por los interesados en hacerlo.

INTRODUCCIÓN

Actualmente, y en todo el mundo, Internet, o más ampliamente las redes IP, junto con la telefonía móvil son los dos fenómenos que captan mayor interés dentro del mundo de las telecomunicaciones, y prueba de ello es el crecimiento experimentado en el número de usuarios que están por utilizar estos dos servicios.

La utilización de la telefonía sobre IP como sustituto de la telefonía convencional se debe, principalmente, a su reducido costo. Sin embargo, existen estudios que demuestran que el nivel de costos de los dos tipos de tecnologías (conmutación de circuitos y voz sobre IP) no es realmente determinante para la tarifa final que paga el cliente. En otras palabras, los operadores tradicionales de tráfico de larga distancia y tradicional podrían, y seguramente lo harán, bajar los precios de forma que se llegue a un nivel de costo similar para una misma calidad de voz. Se prevé por tanto que sólo durante un período de cinco años existirán argumentos económicos en favor de la voz sobre IP.

Después de este período, serán otros argumentos los que favorezcan la utilización de técnicas de telefonía sobre IP, como son la posibilidad de multimedia, control del enrutamiento por parte del PC del usuario, unificación absoluta de todos los medios de comunicación en un sólo buzón, creación de nuevos servicios, etc.

Este tipo de servicios es nuevo, en el sentido que realmente no son simples sustitutivos de servicios existentes. Por esta misma razón no es fácil predecir la evolución del mercado en este segmento. También es impredecible la cantidad de nuevos servicios que pueden surgir cuando uno de los extremos de la llamada, al menos, es un PC que a su vez está sujeto a una evolución tremenda.

1. JUSTIFICACIÓN

En la actualidad las comunicaciones están avanzando a grandes velocidades y con grandes innovaciones a nivel digital y comunicación inalámbrica. Sin embargo, las empresas que manejan el monopolio y la columna vertebral de las comunicaciones son muy celosas y cuidadosas con el uso de ellas. Por esta razón, los avances tecnológicos que ofrecen excelentes servicios en economía y calidad no pueden ponerse a disposición de los usuarios ya que representan una amenaza económica para estas empresas.

El protocolo SIP es un desarrollo que ya esta muy avanzado pero que por los motivos mencionados no se ha podido comercializar, hay leyes que lo prohíben y limitan legalmente. Lo que está permitido es prestar este servicio a las compañías que cuentan con redes internas y que solo las utilizan para transporte de datos y otras pocas aplicaciones, desconociendo las grandes ventajas que podrían obtener sin hacer una gran inversión, pues lo mas importante ya lo tienen: la infraestructura de red.

Lo único que queda para implementar un servidor SIP y prestar el servicio de Voz sobre IP es instalarlo, configurarlo y adquirir los terminales de usuario mencionados anteriormente. El beneficio principal de un servicio de VoIP[1] es el ahorro en dinero que representan las comunicaciones a través de IP y la versatilidad del las aplicaciones y funciones que se pueden obtener a través de este protocolo.

[1] Voz sobre IP. Método de envío de voz por redes IP.

2. PLANTEAMIENTO DEL PROBLEMA

En el momento las comunicaciones telefónicas se realizan a través de grandes plantas telefónicas interconectadas que conmutan las llamadas entre usuarios. Inicialmente el servicio de Internet a nivel de usuario fue prestado a través del cableado telefónico utilizando solo una pequeña parte (4KHz) de su ancho de banda; pero ahora con la gran acogida y proyección que ha tenido en el mundo los servicios de Internet de banda ancha (Cable MODEM[2], DSL[3], etc.) se han desarrollado protocolos muy flexibles y robustos para enrutar comunicaciones telefónicas a través del protocolo de Internet (IP) que no se pueden pasar por alto, siendo estos sistemas, la tendencia unísona para bajar costos en el servicio telefónico, ampliar capacidad de contenidos, disminuir sustancialmente la infraestructura necesaria para telefonía fija y permitir una flexible ínter-conectividad entre sistemas fijos y móviles a bajo costo.

Básicamente el problema es el alto costo del servicio telefónico actual y la baja capacidad de contenidos del mismo con respecto a las soluciones tecnológicas que se exponen en este documento.

[2] Dispositivo que permite tener acceso a datos a muy alta velocidad mediante una conexión CATV.
[3] Línea de suscripción digital.

3. OBJETIVOS

3. 1 OBJETIVO GENERAL

Instalación y configuración de un servidor SIP *(Session Initiation Protocol)*.

3. 2 OBJETIVOS ESPECÍFICOS

Conocer cada una de las etapas presentes en una comunicación entre usuarios establecida a través del protocolo SIP.

Conocer las especificaciones técnicas para la implementación de un servidor SIP.

Instalar y configurar un servidor SIP de prueba para comunicaciones dentro de la red de área local de la Universidad Autónoma de Occidente.

Configurar e instalar las terminales de usuario SIP, ya sean SIP hardphones o aplicaciones de software para su uso eficiente dentro del sistema.

4. ANTECEDENTES

EL protocolo SIP fue desarrollado inicialmente por la IETF (Internet Engieneering Task Force) como un Internet-Draft [4]en 1997 en su versión 1.0. Mas adelante en 1998 desarrollaron la versión 2.0 también como un Internet-Draft en 1998, y en 1999 fue publicada como un RFC[5] (Request For Comments). De ahí en adelante es compromiso de la IETF seguir en el desarrollo de este protocolo.

Existe un protocolo más antiguo conocido como H.323 de la UIT (Unión Internacional de Telecomunicaciones) para trabajar multimedia sobre IP, parecido al SIP, que busca la Voz sobre IP. Este ha estado desde 1996 pero ahora esta siendo reemplazado por el SIP. Dentro de este protocolo esta el H.225 encargado de la señalización y el H.245 encargado de la capacidad de intercambio de información multimedia.

El H.323 es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan la entrega de calidad de servicio (QoS). Algunos ejemplos son TCP/IP e IPX sobre Ethernet, Fast Ethernet o Token Ring. La tecnología de red más común en la que se está implementando el H.323 es IP (Internet Protocol).

[4] Documento no oficial o borrador que se pone a disposición pública para recibir todas las recomendaciones y correcciones antes de ser un RFC.
[5] Serie de documentos que describen el conjunto de protocolos de Internet y experimentos similares.

Este estándar define un amplio conjunto de características y funciones. Algunas son necesarias y otras opcionales. El H.323 define mucho más que los terminales. El estándar define componentes como: terminales, Gateways[6], Gatekeepers[7] y unidades de control Multipunto.

El H.323 utiliza los mismos algoritmos de compresión para el vídeo y el audio que se describen en la norma H.320, aunque introduce algunos nuevos. Se utiliza T.120 para la corroboración de datos.

Anteriormente al H.323, ITU se enfocó exclusivamente en la estandarización de las redes globales de telecomunicaciones. Por ejemplo, en 1985 se comenzó el trabajo en la especificación que define el envío de imagen y voz sobre redes de circuitos conmutados, tales como RDSI. La ratificación de la norma H.320 tuvo lugar 5 años después (fue aprobada por el CCITT en Diciembre de 1990). Sólo 3 años después se dispuso de equipos que cumplieran con la norma y que permitieran la interoperabilidad entre sí.

En Enero de 1996, un grupo de fabricantes de soluciones de redes y de ordenadores, propuso la creación de un nuevo estándar ITU-T para incorporar videoconferencia en redes de área local. Inicialmente, las investigaciones se centraron en las redes de área local siendo éstas más fáciles de controlar. Sin embargo, con la expansión del Internet, el grupo tuvo que incluir todas las redes IP dentro de una única recomendación, lo cual marcó el inicio del H.323.

[6] Pasarela entre dos redes.

[7] Es la unidad central de control que gestiona las prestaciones en una red de Voz o Fax sobre IP, o de aplicaciones multimedia y de videoconferencia.

El H.323 soporta vídeo en tiempo real, audio y datos sobre redes de área local, metropolitana, regional o de área extensa. Soporta así mismo Internet e Intranet. En Mayo de 1997, el Grupo 15 del ITU redefinió el H.323 como la recomendación para los sistemas multimedia de comunicaciones en aquellas situaciones en las que el medio de transporte sea una red de conmutación de paquetes que no pueda proporcionar una calidad de servicio garantizada.

H.323 también soporta videoconferencia sobre conexiones punto a punto, telefónicas y RDSI. En estos casos, se debe disponer un protocolo de transporte de paquetes tal como PPP.

De cualquier manera, estos desarrollos no se han podido implementar en países como Colombia en las redes telefónicas públicas de usuarios como elemento principal y queda entonces esta tecnología a disposición de las empresas que decidan hacer la inversión, que no es muy alta en relación con los grandes ahorros en gastos de operación que este tipo de sistemas significa.

5. MARCO TEÓRICO

5. 1 SIP (PROTOCOLO DE INICIALIZACIÓN DE SESIÓN)

5. 1. 1 Introducción. Hay muchas aplicaciones en el Internet que requieren el manejo de una sesión, donde una sesión es considerada un intercambio de datos entre una asociación de participantes. La implementación de estas aplicaciones es complicada dependiendo de los participantes. Los usuarios pueden moverse a cualquier sitio, pueden tener varias direcciones o nombres asociados y pueden establecer comunicaciones sobre distintos medios; algunas veces simultáneamente. Se han desarrollado numerosos protocolos que transportan sesiones multimedia en tiempo real como voz, vídeo o mensajes de texto. El protocolo de inicialización de sesión funciona en paralelo con estos protocolos permitiendo a los usuarios en el Internet descubrir la ubicación del otro y definir la sesión que se quiere inicializar. Desde la perspectiva de localización de sesión de los participantes, y otras funciones, el protocolo SIP permite la creación de una infraestructura de servidores proxy a los cuales los usuarios pueden mandar peticiones de registro y de invitación a sesión. El protocolo SIP es una herramienta ágil de propósito general que permite crear, modificar y terminar sesiones que funcionan independientemente del protocolo y sin importar el tipo de sesión que se esté estableciendo.

5. 1. 2 Funcionalidad del protocolo SIP. El protocolo SIP es un protocolo de control de la capa de aplicación que puede establecer, modificar y terminar sesiones multimedia como las llamadas telefónicas a través del Internet. Este protocolo permite además invitar participantes a una sesión ya existente; un

ejemplo de esto son las conferencias multicast. Datos multimedia pueden ser añadidos o removidos de una sesión existente. El protocolo SIP soporta transparencia de mapeo de nombres y servicios de redirección, lo cual significa que los usuarios pueden tener un identificador externo único sin importar su ubicación en la red.

El protocolo SIP permite 5 facetas de establecimiento y terminación de comunicaciones multimedia.

- **Localización de usuarios.** Determina el punto final con el que se va a establecer la sesión.
- **Disponibilidad de usuarios.** Determina la disponibilidad del destino para iniciar una sesión.
- **Capacidad de usuario.** Determina los parámetros y el tipo de multimedia que se va usar.
- **Configuración de sesión.** Establecimiento de los parámetros de la sesión para la fuente y el destino de la llamada.
- **Manejo de sesión.** Transferencia y terminación de sesión, modificación de parámetros de sesión y configuración de servicios.

El protocolo SIP no es un sistema de comunicación integrado verticalmente, es más un componente que puede ser utilizado con otros protocolos de la IETF para adecuarse a cualquier arquitectura multimedia. Típicamente, estas arquitecturas incluyen protocolos como el RTP para transportar datos en tiempo real con retroalimentación de calidad de servicio (QoS), el RTCP para controlar la entrega de datos multimedia muestreados, el protocolo MEGACO[8] para controlar el acceso a la Red Telefónica Pública Conmutada (PSTN) y el

Protocolo de Descripción de Sesión (SDP) para describir sesiones multimedia. Así el protocolo SIP debe ser usado en conjunto con otros protocolos para proveer servicios completos a los usuarios. Sin embargo, la funcionalidad y operación básica del protocolo SIP no depende de ninguno de estos protocolos.

El protocolo SIP no provee servicios, en vez de esto, provee premisas que pueden ser usadas para implementar diferentes servicios. Por ejemplo, SIP puede localizar usuarios y entregar un objeto opaco a su localización actual. Si esta primitiva es usada para entregar una descripción de sesión escrita en SDP, los terminales de usuario pueden acceder a los parámetros de la sesión.

El protocolo SIP no ofrece servicios de control de conferencias y no prescribe cómo debe ser manejada una conferencia. SIP puede ser usado para inicializar una sesión de conferencia que usa otros protocolos de control. Como los mensajes SIP y sus sesiones pueden pasar a través de distintas redes, SIP no puede y no lo hará, proveer ninguna clase de características de control de recursos en una red.

La naturaleza de los servicios prestados hace que la seguridad sea particularmente un parámetro importante. Para tal fin, el protocolo SIP posee una serie de características de seguridad, las cuales incluyen autentificación de sesión, protección de integridad, encriptación y servicios de privacidad. Este protocolo funciona tanto con la versión IPv4 como con la versión IPv6 del protocolo de Internet.

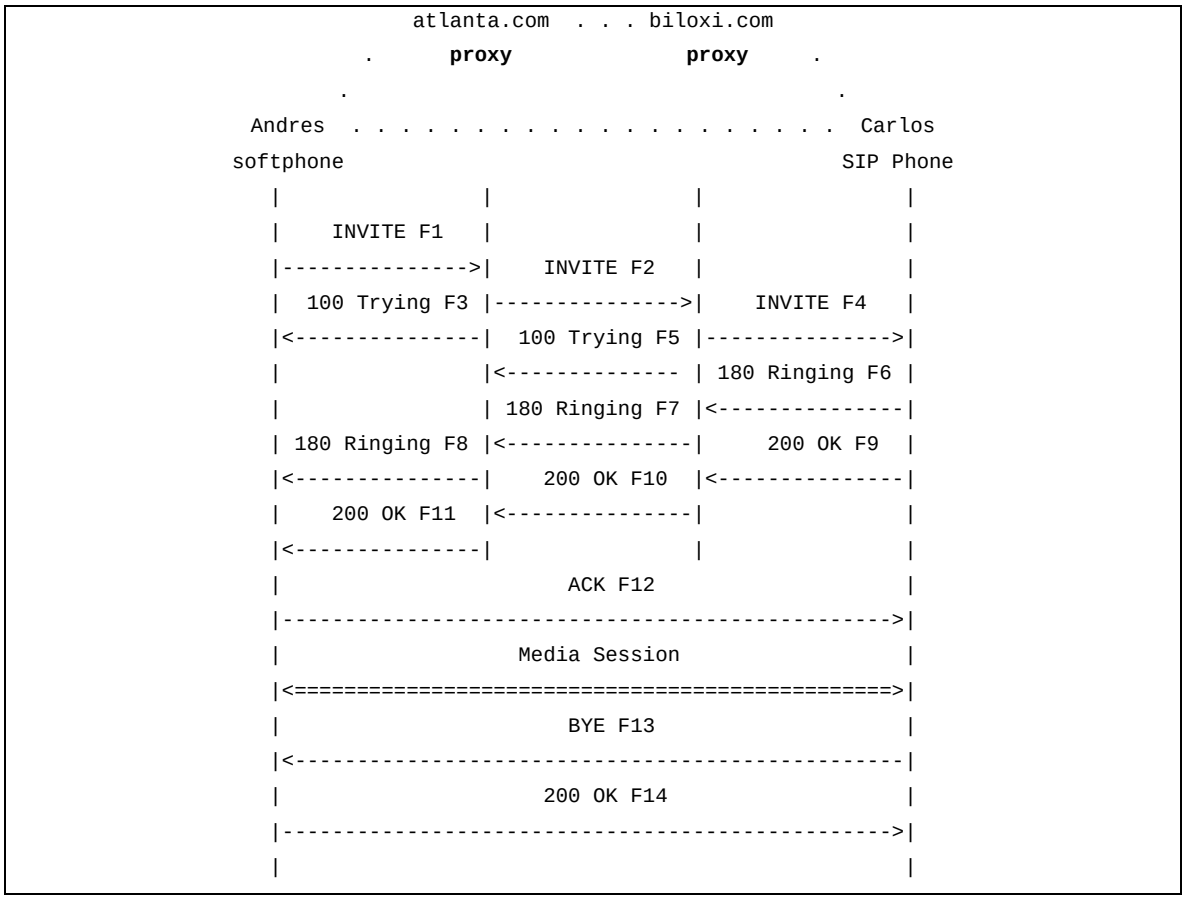
[8] Control de Pasarela de Medios.

5. 1. 3 Operación del SIP. A continuación se explicará el funcionamiento del protocolo por medio de un ejemplo básico de operación el cual hará más fácil el entendimiento del comportamiento de este protocolo en una red. El ejemplo mostrará las funciones básicas del protocolo: la localización de un usuario, la señalización necesaria para comunicar, negociar y establecer los parámetros para iniciar una sesión, y la terminación de la misma una vez ya establecida.

En la figura 1 se muestra un ejemplo típico de un intercambio de mensajes SIP entre dos usuarios, Andrés y Carlos. En este ejemplo, Andrés utiliza una aplicación SIP en su Pc (softphone) para llamar a Carlos a su teléfono SIP a través del Internet. Además se muestran dos servidores proxy que actúan en medio de Andrés y Carlos para facilitarles el establecimiento de la sesión. Este arreglo típico se conoce como SIP trapezoidal.

Andrés llama a Carlos utilizando su identidad SIP, un tipo de recurso de identidad uniforme llamado SIP URI. Estos SIP URIs son similares a la dirección de correo electrónico típicamente contienen un nombre de usuario y el nombre del dominio del servidor. En este caso es sip:carlos@biloxi.com, donde biloxy.com es el dominio del servidor SIP en el cual se encuentra suscrito Carlos. El SIP URI de Andrés es sip:andres@atlanta.com. Andrés puede llamar a la dirección URI de Carlos o quizás hacer un click sobre el hipervínculo en la libreta de direcciones. SIP también provee una dirección URI segura llamada SIPS URI. Un ejemplo de este tipo dirección sería sips:andres@biloxy.com. Una comunicación por medio de una URI segura garantiza un transporte cifrado y seguro llamado TLS y es usado para transportar todos los mensajes SIP desde la fuente hacia el dominio del destino. De ahí, el pedido es mandado de forma segura al destino, pero con un mecanismo de seguridad que depende de las políticas de seguridad del dominio del usuario destino.

Figura 1. Esquema SIP trapezoidal



Fuente : SIP : Session Initiation Protocol [en línea]. East Hanover : Network Working Group, 2002. [Citado 1 de feb 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3261.txt.

El protocolo SIP está basado en un modelo de transacción de pedido y respuesta parecido al HTTP[9]. Cada transacción consiste en un pedido que invoca a un método o función en particular en el servidor y al menos una respuesta. En este ejemplo, la transacción comienza cuando el teléfono de Andrés envía un pedido de invitación hacia Carlos. El pedido de invitación *INVITE* es un ejemplo de un método SIP que especifica una acción que la

[9] Protocolo de transporte de Hipertexto.

fuente (Andrés) desea que el destino (Carlos) reciba. El pedido de invitación contiene un número de campos de cabecera, estos son llamados atributos, los cuales proveen información adicional acerca del mensaje. Estos campos presentes en una petición de invitación incluyen un identificador único de la llamada, la dirección del destino, la dirección de la fuente y la información acerca del tipo de sesión que Andrés desea establecer con Carlos. A continuación se muestra este mensaje de invitación.

Figura 2. Mensaje de invitación 1

```
INVITE sip:carlos@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Carlos <sip:carlos@biloxi.com>
From: Andres <sip:andres@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:andres@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

Fuente: SIP : Session Initiation Protocol [en línea]. East Hanover : Network Working Group, 2002. [Citado 1 de feb 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3261.txt.

La primera línea del mensaje contiene el nombre del método *INVITE*. Las líneas siguientes son una lista de campos de cabecera. Este ejemplo contiene un juego mínimo de campos requeridos. Los campos de cabecera serán descritos a continuación.

- **Via**. Este campo comienza con un pequeño encabezado con el nombre del protocolo, la versión y el protocolo de transporte. Además contiene la dirección (pc33.atlanta.com) en la cual Andrés está esperando recibir

respuesta a su petición. También contiene parámetros que identifican la transacción.

- **To**. Contiene un nombre de despliegue (Carlos) y el SIP o SIPS URI (sip:carlos@biloxy.com) donde el pedido fue originalmente direccionado.

- **From**. También contiene el nombre de despliegue (Andrés) y el SIP o SIPS URI que indica quien originó el pedido (sip:andres@atlanta.com). Este campo además cuenta con una etiqueta que contiene una cadena aleatoria de caracteres alfanuméricos la cual fue generada por el **softphone** de Andrés; esta es usada para propósitos de identificación.

- **Call-ID**. Contiene un indicador global único para la llamada, generado por la combinación entre una cadena aleatoria y el nombre del Host [10]o la dirección IP[11] de softphone.

- **Cseq**. El comando de secuencia contiene un entero y el nombre del método. Este número se incrementa cada vez que hay un nuevo pedido en el diálogo y tradicionalmente se incrementa secuencialmente.

- **Contact.** Usualmente se compone del nombre de usuario y el nombre de dominio totalmente calificado o FQDN. Se prefiere el uso de un FQDN pero muchos usuarios no tienen registrados nombres de dominio, así que se permite poner la dirección IP de la máquina. Mientras que el

[10] Es un ordenador directamente conectado a una red que efectúa las funciones de un servidor y alberga servicios.

campo **Via** le dice a los otros elementos donde manda la respuesta, el campo de contacto le dice al otro elemento donde mandar futuras peticiones.

- **Max-Frowards.** Sirve como un limitante del número de saltos que un pedido puede hacer hacia su destino que consiste en un número entero el cual es decrementado en cada salto que el paquete realiza.

- **Content-Type.** Contiene una descripción del campo del mensaje (no se muestra).

- **Content-Length.** Contiene el conteo de caracteres en el cuerpo del mensaje.

Los detalles de una sesión, como el tipo de medio, codec[12], o rata de muestreo, no son descritos usando SIP. Preferiblemente el cuerpo del mensaje contiene la descripción de la sesión, codificada en algún otro formato de protocolo. Uno de estos formatos es el protocolo descripción de sesión (SDP). Este mensaje es transportado por el mensaje SIP análogamente a un archivo adjunto que es mandado en un correo electrónico, o una página Web que es transportada por un mensaje HTTP.

Como el softphone de Andrés no conoce la ubicación de Carlos o del servidor SIP del dominio biloxi.com, este manda un mensaje de invitación al servidor

[11] Código numérico que es asignado a un ordenador o equipo específico en el Internet.
[12] Algoritmo software usado para comprimir y descomprimir señales de voz o audio.

que provee el servicio de VoIP a Andrés (atlanta.com). La dirección del servidor SIP atlanta.com pudo haber sido configurada en el softphone de Andrés, o pudo ser descubierta usando por ejemplo DHCP[13].

El dominio atlanta.com contiene un tipo de servidor conocido como *servidor proxy*[14], el cual recibe el pedido SIP y lo envía como si él fuera la fuente. En este ejemplo el servidor proxy recibe el pedido de invitación y envía una respuesta *100 Trying* de vuelta para indicar que el mensaje fue recibido, se está procesando y se está enrutando hacia su destino.

Las respuestas en el protocolo SIP usan un código de tres dígitos seguido por una línea de descripción. Esta respuesta contiene exactamente los mismos mensajes de cabecera que se enviaron anteriormente para qué el softphone los compare. El servidor atlanta.com localiza el servidor biloxy.com posiblemente a través de un servicio de nombres de dominio para buscar el servidor SIP en el dominio biloxy.com. Como resultado se obtiene la dirección IP del servidor proxy de biloxy.com y se direcciona el mensaje de invitación hacia este. Antes de enviar el pedido, el servidor proxy de atlanta.com añade un valor adicional en la cabecera Via que contiene su propia dirección IP además de la dirección IP de Andrés. El servidor proxy de biloxy.com recibe la invitación y le responde con un *100 Trying* al servidor proxy de atlanta.com para indicarle que el mensaje fue recibido y que se está procesando el pedido. El servidor proxy de biloxy.com añade un valor adicional a la cabecera Via del mensaje de invitación con su propia dirección IP y luego lo envía al teléfono SIP de Carlos. El teléfono SIP de Carlos recibe la petición de invitación y alerta a Carlos de la llamada entrante de Andrés, así que Carlos puede decidir si recibe o no la llamada; esto significa que el teléfono empieza a repicar. El

[13] Protocolo de Configuración Dinámica del equipo.
[14] Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada.

teléfono SIP de Carlos indica esto con una respuesta *180 Ringing*, la cual es enrutada a través de los dos servidores proxy hacia el teléfono de software de Andrés. Cada servidor usa la información que hay en el campo de cabecera Via para determinar donde enviar la respuesta y remueve de el su propia dirección IP. Como resultado, la respuesta *180 Ringing* puede ser enviada hacia el teléfono de software de Andrés sin ser procesada por los servidores proxy. Esto es bastante positivo ya que cada servidor proxy ve el mensaje de invitación y además la respuesta a este mensaje, permitiendo al administrador detectar alguna falla o comprobar el correcto funcionamiento del servicio.
Cuando el teléfono de software de Andrés recibe la respuesta *180 Ringing*, le pasa esta información a el, quizás usando un tono de sonido mostrándole un mensaje en la pantalla del ordenador.

En este ejemplo, Carlos decide atender al teléfono. Cuando levanta el auricular, su teléfono SIP envía una respuesta *200 OK* (Figura 3) lo cual indica que la llamada ha sido atendida. Esta respuesta contiene un campo de mensaje con la descripción SDP del medio y el tipo de sesión que Carlos está dispuesto a establecer con Andrés. Como resultado hay dos fases de intercambio de mensajes SDP: Andrés envía uno a Carlos, y Carlos envía uno de vuelta a Andrés. Este intercambio de dos fases provee una negociación básica de las capacidades de cada uno y está basado en un modelo general de oferta y demanda del intercambio SDP. Si Carlos no desear atender la llamada o está ocupado con otra, una respuesta de error es enviada en vez de la respuesta *200 OK.*

Figura 3. Mensaje de respuesta 1

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP server10.biloxi.com
;branch=z9hG4bKnashds8;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com
```

```
;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com
;branch=z9hG4bK776asdhds ;received=192.0.2.1
To: Carlos <sip:carlos@biloxi.com>;tag=a6c85cf
From: Andres <sip:andres@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:carlos@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131
```

Fuente: SIP : Session Initiation Protocol [en línea]. East Hanover : Network Working Group, 2002. [Citado 1 de feb 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3261.txt.

La diferencia en este mensaje (Figura 3) radica en el campo Via el cual contiene la información que ha insertado cada uno de los servidores proxy. Cuando el mensaje llega al teléfono de software de Andrés éste deja de repicar, indicando que la llamada ha sido contestada. Finalmente el teléfono de Andrés envía un mensaje *ACK* al teléfono de Carlos para confirmar la recepción de la respuesta *200 OK*. En este ejemplo, el mensaje *ACK* es enviado directamente del teléfono de Andrés al teléfono de Carlos a través de los dos servidores proxy. Esto ocurre gracias a que los terminales de usuario han registrado la dirección de cada uno la cual han extraído del campo de cabecera Contact de los mensajes *INVITE/200 OK*. Estas direcciones eran desconocidas cuando el primer mensaje de invitación no había sido enviado. Esto significa que los servidores proxy ya no son necesarios para la comunicación y el flujo de la llamada no pasa a través de ellos. Esto completa el entendimiento de tres vías que se necesita para establecer sesiones por medio del protocolo SIP.

En este momento la sesión multimedia entre Andrés y Carlos se inicia, y los teléfonos de cada uno envían paquetes multimedia usando el formato que los

dos han aceptado en el intercambio SDP. En general los paquetes entre los dos usuarios toman una ruta diferente a los paquetes de señalización SIP.

Durante la sesión tanto Carlos como Andrés pueden decidir cambiar las características multimedia de esta. Esto les significa mandar un paquete de re-invitación que contiene el nuevo tipo de información multimedia que se desea utilizar. Este paquete pertenece al diálogo ya existente, así que el otro usuario entiende que esta petición se refiere a una re-configuración de la sesión en vez del establecimiento de una nueva. Si el otro usuario acepta el paquete de re-configuración o re-invitación, entonces envía un código *200 OK* aceptando el cambio y el usuario que pide la re-configuración de sesión le responde con un mensaje *ACK*. Si por el contrario, la contraparte no acepta el cambio o es incapaz de hacerlo ya que no posee por ejemplo el tipo de codec al que se desea cambiar, envía un mensaje de error con el código *488 Not Acceptable Here* el cual también recibe un mensaje *ACK* como respuesta al teléfono que hizo la petición. Lo anterior no significa que la sesión se finaliza, sino que continúa utilizando el tipo de sesión anteriormente negociado.

Al final de la llamada, Carlos se desconecta primero al colgar el teléfono, esto conlleva a que un mensaje *BYE* sea enviado. Este mensaje es enviado directamente al teléfono de Andrés, otra vez pasando a través de los servidores proxy. Andrés confirma la recepción de este último mensaje con una respuesta *200 OK*, lo cual termina la sesión y las transacciones de mensajes SIP. En algunos casos, esto puede ser útil para los servidores proxy en la señalización del camino del SIP para ver toda la transferencia de mensajes entre los usuarios durante el tiempo en que la sesión éste activa.

El registro es otra operación bastante común y crucial en el protocolo SIP. El acto de registrarse es la forma que tiene el servidor biloxi.com de saber la ubicación actual de Carlos. En la inicialización y en intervalos periódicos de tiempo, el teléfono SIP envía mensajes de registro al servidor de dominio conocido como **"**SIP registrar[15]**"**. El mensaje *REGISTER* asocia la dirección SIP URI con la máquina en la cual se está registrando el teléfono SIP. El servidor de registro almacena esta asociación, lo cual es también llamado "binding[16]", en una base de datos llamada *servicio de ubicación*, la cual puede ser usada por el servidor proxy para saber la ubicación de sus usuarios registrados.

Comúnmente, el servidor de registro de un dominio está configurado en la misma máquina donde está el servidor proxy para ese dominio. Este es un concepto importante en la distinción entre los tipos de servidores SIP ya que esta es lógica más no física.

Carlos no está limitado a registrarse desde un solo dispositivo. Por ejemplo, él puede tener un teléfono SIP tanto en casa como en su oficina los cuales están en la capacidad de enviar mensajes de registro utilizando el mismo número telefónico o nombre de usuario. Esta información es guardada en el servicio de ubicación y le permite el servidor proxy ejecutar varios tipos de búsquedas para ubicar a Carlos. Similarmente, más de un usuario puede estar registrado en un solo dispositivo al mismo tiempo.

El servicio de ubicación es justamente un concepto muy abstracto. Generalmente contiene información que le permite al servidor proxy introducir al servidor de ubicación una dirección URI y recibir cero o varias direcciones

[15] Servidor para el registro de usuarios SIP en línea.
[16] Ligamento o enlace entre direcciones y/o puertos IP y máquinas dentro de una red.

URI que le dicen a donde mandar la petición. La acción de registro es una vía para crear esta información, pero no la única. Funciones arbitrarias de mapeo pueden ser configuradas a discreción del administrador del servicio de telefonía SIP.

Finalmente, es importante anotar que en el protocolo SIP, la acción de registros es usada para enrutar todos los mensajes y peticiones SIP entrantes; lo cual no tiene ningún rol autorizando mensajes de salida. La autorización y la autentificación son manejadas por el protocolo SIP en una base de pedido por pedido con un mecanismo de acción y reacción, o usando un esquema en la capa física.

5. 1. 4 Mensajes SIP. SIP es un protocolo basado en texto y utiliza un juego de caracteres UTF-8. Un mensaje SIP puede ser un pedido de un cliente al servidor o una respuesta de un servidor al cliente. Los mensajes de pedido y respuesta utilizan el formato básico descrito en el RFC 2822, aunque la sintaxis difiere en el juego de caracteres y las especificaciones de sintaxis. Ambos tipos de mensajes consisten de una línea de inicio, cero o más campos de cabecera, una línea vacía indicando el fin de los campos de cabecera y un cuerpo de mensaje el cual es opcional.

Figura 4. Formato de cabecera RFC 2822

```
Mensaje genérico = Línea de inicio
                        *cabecera del mensaje
                         CRLF
                         [cuerpo del mensaje]
     Línea de inicio  = Línea de pedido / Línea de estado
```

Fuente: SIP : Session Initiation Protocol [en línea]. East Hanover : Network Working Group, 2002. [Citado 1 de feb 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3261.txt.

La línea de inicio, cada línea del encabezado y la línea vacía deben terminar con una secuencia de retorno de carro y de cambio de línea (CRLF). En el diagrama anterior se debe tener en cuenta que aunque el cuerpo del mensaje sea vacío la línea en blanco debe estar siempre presente.

- **Pedidos SIP**. Los mensajes de pedido contienen una línea de pedido en la línea de inicio. La línea de pedido contiene el nombre del método, el URI de pedido y la versión del protocolo separada por un espacio simple.

  - **Métodos SIP**. Esta especificación define seis métodos; *REGISTER* para registrar la información de los contactos, *INVITE*, *ACK*, y *CANCEL* para configurar e inicializar sesiones, *BYE* para terminar sesiones y *OPTIONS* para preguntar a los servidores sus capacidades. Las extensiones SIP pueden definir métodos adicionales.

  - **Request-URI**. Indica el usuario del servicio al cual está siendo enviado este pedido.

  - **SIP-Version**. Los mensajes de respuesta y de pedido incluyen la versión del SIP que se está utilizando.

- **Respuestas SIP**. La respuesta SIP se distingue de los pedidos porque tiene una línea de estado como línea de inicio. La línea de estado consiste en la versión del protocolo seguida por un código de estado numérico y es asociada en una frase textual con cada elemento separado por un espacio.

- **Códigos de estado**. El código de estado es un entero de tres dígitos que indica la salida de un intento para entender y satisfacer un pedido. Este código está relacionado para que el usuario humano pueda entender el estado real de las transferencias SIP.

  El primer dígito del código de estado define la clase de respuesta. Los últimos dos dígitos no tienen ninguna categorización. Por esta razón, cualquier respuesta con un código entre 100 y 199 se refiere como una respuesta *1xx* y así sucesivamente. El protocolo SIP/2.0 permite seis valores para el primer dígito. Esta descripción se ilustra en la Figura 5.

Figura 5. Descripción de códigos de estado

1xx: Provisional -- ha sido recibido el pedido, se continúa a procesarlo.
2xx: Éxito -- la acción fue recibida exitosamente, comprendida y aceptada.
3xx: Redirección -- más acciones se deben tener en cuenta para completar el pedido.
4xx: Error del cliente -- el pedido contiene una sintaxis errónea o no puede ser procesada por el servidor.
5xx: Error del servidor -- el servidor ha fallado en procesar un pedido aparentemente válido.
6xx: Falla global -- el pedido no puede ser procesado por ningún servidor.

Fuente: SIP : Session Initiation Protocol [en línea]. East Hanover : Network Working Group, 2002. [Citado 1 de feb 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3261.txt.

A continuación se mostrarán todos los códigos de estado y su significado.

Tabla 1. Códigos de estado SIP

CODIGO	SIGNIFICADO
100	Trying
180	Ringing
181	Call Is Being Forwarded
182	Queued
183	Session Progress
200	OK
202	OK
300	Multiple Choices
301	Moved Permanently
303	See Other
305	Use Proxy
380	Alternative Service
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
413	Request Entity Too Large
414	Request-URI Too Large
415	Unsupported Media Type
420	Bad Extension
480	Temporarily not available
481	Call Leg/Transaction does not exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete

CODIGO	SIGNIFICADO
485	Ambiguous
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
489	Bad Event
491	Request Pending
493	Undecipherable
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Time-out
505	SIP Version not supported
513	Message Too Large
580	Precondition Failure
600	Busy Everywhere
603	Decline
604	Does Note Exist Anywhere
606	Not Acceptable

5. 2 RTP (PROTOCOLO DE TRANSPORTE EN TIEMPO-REAL)

5. 2. 1 Introducción. Esta sección específica el protocolo de transporte para tiempo real RTP, el cual provee servicios de entrega punto a punto para aplicaciones que tengan características de tiempo real, así como vídeo y audio interactivo. Estos servicios incluyen identificación de tipo de contenido, numeración de secuencia, marca de tiempo y monitoreo.

Las aplicaciones por lo general corren RTP sobre UDP[17] para hacer uso de sus servicios de multiplexado [18]y checksum[19], de esta manera ambos protocolos contribuyen parte a la funcionalidad del protocolo de transporte. Como sea, RTP debe ser usado con otros protocolos de la capa de red o de transporte. RTP soporta transporte de datos para múltiples destinos usando difusión multicast si proviene de la capa de red.

Nótese que RTP por sí mismo no provee ningún mecanismo para asegurar entregas oportunas o para proveer otras garantías de calidad de servicio, pero se apoya en servicios de capas inferiores para hacerlo. RTP no garantiza entregas o prevención de entrega fuera de orden, y tampoco asume que la capa de red es confiable y entrega paquetes en secuencia. Los números de secuencia incluidos en RTP permiten al receptor reconstruir la secuencia de los paquetes enviados. Además, esta puede ser usada para determinar la localización correcta de un paquete, por ejemplo en decodificación de video, ya que puede decodificarlos en desorden y después reproducirlo en el orden adecuado según los números de secuencia.

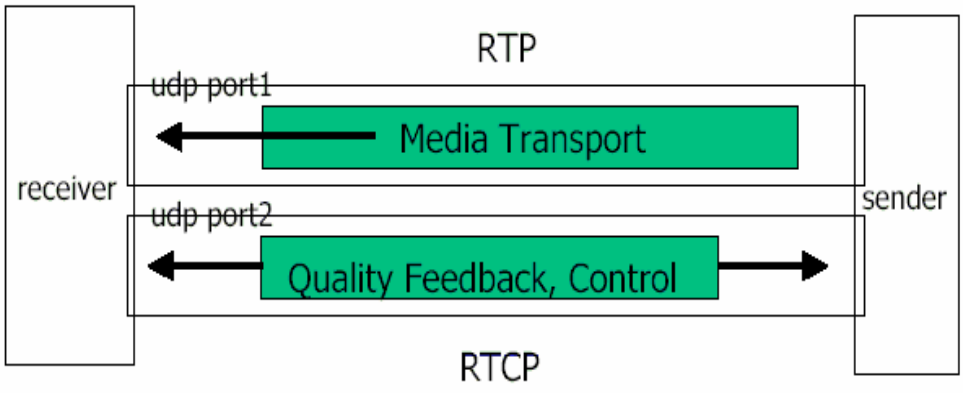
El RTP en principio fue diseñado para satisfacer la necesidad de múltiples usuarios en conferencias Multimedia. Pero este no se limita solo a esta aplicación, almacenamiento de datos continuos, simulación distribuida interactiva y aplicaciones de medición y control pueden encontrar aplicable el RTP. El RTP consiste en dos partes estrechamente ligadas.

[17] Protocolo de Datagramas de Usuario.
[18] Método por el cual mediante un algoritmo, implementado en hardware o software, se puede transmitir algún tipo de información especifica por un mismo canal compartido.
[19] Suma de chequeo. Sirve para evaluar si al información que contiene un paquete de red es la correcta.

- El protocolo de Transporte en Tiempo Real (RTP), para llevar datos que tengan propiedades de tiempo Real.

- Y el Protocolo RTP de Control (RTCP), para monitorear la calidad del servicio y para convenir información sobre los participantes de la sesión en curso.

Figura 6. Esquema de funcionamiento del RTP/RTCP



Fuente: Voice Over IP [en línea]. New York : Prorocols.com Group, 2003. [Citado 05 de feb, 2004]. Disponible por internet : www.protocols.com/pbook/ VoIPFamily.htm.

RTP representa un nuevo estilo de protocolos siguiendo los principios del esquema de nivel de aplicación. Fue propuesto para ser manipulado y para proveer la información requerida por una aplicaron particular.

5. 2. 2 Escenarios de uso del protocolo RTP.

- **Audio Conferencia para Multiusuarios Simple**. Los usuarios obtienen un grupo de direcciones multicast y un par de puertos. Un puerto es usado

para el transporte de datos del audio y otro es usado para el control de paquetes (RTCP). Esta información de direcciones y puertos es distribuida entre todos los participantes propuestos para la sesión multiusuario. Si se requiere seguridad, los paquetes de datos y de control deben ser cifrados, en este caso una clave de encriptación debe además ser generada y distribuida.

En la aplicación de conferencia de audio, cada usuario envía datos de audio en pequeños paquetes a una tasa de muestreo de 20 ms. Cada paquete es precedido por un encabezado RTP. Este encabezado y los datos están a su vez en un paquete UDP. El encabezado RTP indica que tipo de codificación de audio esta contenida en cada paquete (PCM[20], ADPCM [21]o LPC[22]), lo cual permite a cada usuario cambiar el tipo de codificación durante la conferencia. Un caso puede darse si un usuario con un enlace de banda angosta desea ingresar a la sesión, o si se debe reaccionar ante congestión en la red.

En el Internet, así como en otras redes por paquetes, ocasionalmente se pierden y reordenan paquetes causando a la transmisión un retraso significativo de tiempo. Para solucionar estos problemas, el encabezado RTP contiene información de tiempos y números de secuencia producidos por la fuente, así en al conferencia de audio, los paquetes son reproducidos cada 20 ms. Esta reconstrucción de tiempo es ejecutada por cada usuario de RTP en la conferencia. El número de secuencia puede también ser usado por el receptor para estimar cuantos paquetes están perdiéndose.

[20] Pulse Code Modulation. Método digital de transmisión de datos análogos mediante la modulación de pulsos codificados.
[21] Adaptative Differencial PCM. Método digital de transmisión de datos análogos mediante algoritmos que detectan la diferencia de información en el tiempo, para disminuir la cantidad de información modulada mediante pulsos codificados.
[22] Linear Predictive Coding. Codificación lineal predictiva.

Como los usuarios pueden entrar y salir durante la conferencia, es muy útil saber quienes están participando en todo momento y que tan bien están recibiendo los datos de audio. Para este propósito, cada participante de la conferencia de audio envía periódicamente un reporte multicast de recepción con el nombre del usuario por el puerto RTCP (Control). Este reporte de recepción indica que tan bien esta recibiendo cada usuario y puede ser usado para controlar codificadores adaptativos.

- **Audio y Video Conferencia**. Si están siendo usados Video y Audio al mismo tiempo en una conferencia, estos son transmitidos como sesiones RTP separadas. Los paquetes RTCP son transmitidos por cada medio usando dos puertos UDP diferentes y/o direcciones multicast. No hay directo acoplamiento en el nivel RTP entre las sesiones de Audio y Video, excepto que la participación del usuario en ambas sesiones deba usar el mismo nombre distintivo (canónico) en los paquetes RTCP, de esta manera las sesiones pueden ser asociadas. Un motivo para esta separación es permitir que algunos participantes en la conferencia reciban un solo medio si lo desean.

- **Mezcladores y Traductores**. En una sesión no es siempre recomendable que todos los participantes manejen el mismo formato de datos de multimedia. En el caso que en una sesión participen usuarios de redes con características distintas de ancho de banda es necesario que haya un intermediario que permita que todos trabajen a la máxima capacidad de su red y no forzar a todos los participantes a trabajar a la taza de transmisión mas baja de la sesión. Este ente intermediario es conocido como Mezclador (Mixer) y se ubica cerca de las redes de banda angosta para re-sincronizar los paquetes de audio entrantes a una tasa de transferencia que esa red pueda trabajar. Después envía los paquetes al usuario en particular o a

varios en forma de multicast. En el caso de que los usuarios tengan disponibilidad de banda ancha pero que se encuentren detrás de un Firewall [23]que no permita que los paquetes ingresen, es decir, que no sean alcanzados por los otros usuarios que están fuera de esa red, es necesario otro intermediario RTP conocido como Traductor. Se instalan dos traductores, uno a cada lado del Firewall. El de afuera pasa todos los paquetes recibidos hacia el traductor de adentro por medio de una conexión segura que el Firewall permita. Luego el Traductor de adentro hace llegar los paquetes a sus destinatarios correspondientes.

5. 2. 3 Definiciones.

- **Tipo de Media RTP**. Es el tipo de datos transportados por el RTP en un paquete, por ejemplo muestras de audio o video comprimido.

- **Paquete RTP**. Es un paquete de datos que consiste en un encabezado RTP fijo, una lista de fuentes contribuyentes (posiblemente vacía), fuentes de sincronismo, fuentes de contribución y los datos multimedia. Algunos protocolos subyacentes pueden requerir un encapsulado del paquete RTP para ser definidos. Típicamente un paquete de un protocolo de nivel inferior contiene un paquete RTP, pero varios paquetes RTP pueden ser contenidos si lo permite el método de encapsulado.

- **Paquete RTCP**. Un paquete de control RTP consiste en un encabezado fijo similar al RTP, seguido por elementos que varían según el tipo de paquete RTCP. Típicamente múltiples paquetes RTCP son enviados en un paquete

[23] Es el método o dispositivo para proteger una red, separándola lógicamente de otra red en la cual no se confía.

único de un protocolo inferior, esto es habilitado por el campo de longitud en el encabezado de cada paquete RTCP.

- **Fuente de sincronización (SSRC)**. Es la fuente de una cadena de paquetes RTP, diferenciada por un identificador numérico SSRC de 32 bits llevada en el encabezado RTP para no depender de la dirección de red. Todos lo paquetes de una fuente de sincronización forman parte de un mismo espacio de tiempo y secuencia. Ejemplos de fuentes sincronizadas puede ser el emisor de una cadena de paquetes derivados de una fuente de señales como un micrófono, una cámara o un mezclador RTP. El identificador SSRC es un valor escogido aleatoriamente para ser globalmente único en una sesión RTP en particular.

- **Fuente de contribución (CSRC)**. Es una de las fuentes de una cadena de paquetes RTP que ha contribuido a la cadena combinada producida por un mezclador RTP. El mezclador inserta una lista de los identificadores SSRC de las fuentes contribuyentes a la generación de un paquete en particular dentro del encabezado RTP de ese paquete.

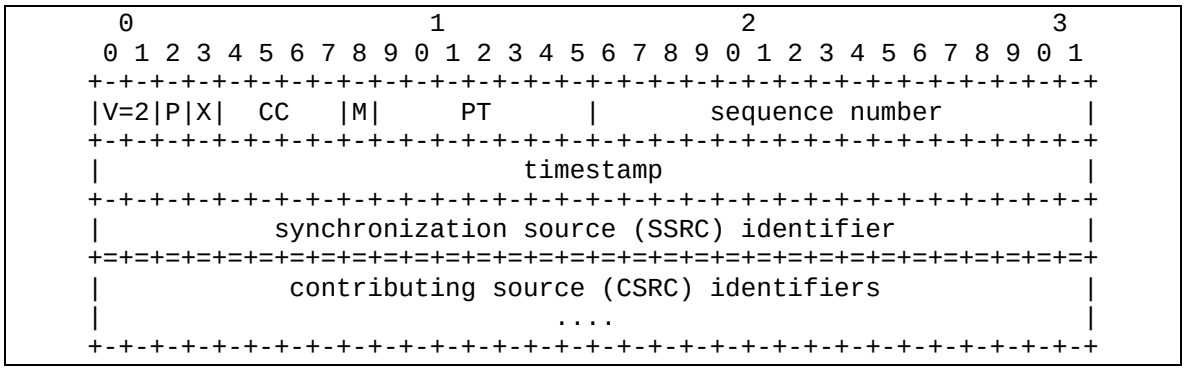
- **Mezclador**. Es un sistema intermediario que recibe paquetes RTP de una o más fuentes, posiblemente cambia los formatos de los datos, combina los paquetes de alguna manera y entonces los envía en un nuevo paquete RTP.

- **Traductor**. Es un sistema intermedio que envía los paquetes RTP con su identificador SSRC intacto. Ejemplos de traductores incluyen dispositivos que convierten codificaciones sin mezclas, replicadores de multicast a unicast, filtros y Firewalls de nivel de aplicación.

5. 2. 4 Cabeceras RTP.

Los primeros 12 octetos son presentados en todo paquete RTP, mientras la lista de los identificadores CSRC es presentada solo cuando es insertado por el mezclador. Los campos tienen el siguiente significado.

Figura 7. Encabezado RTP



RTP : A Transport Protocol for Real-Time Applications [en línea]. Berlin : Network Working Group, 1996. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc1889.txt.

- **Versión (V) - 2 bits**. Este campo identifica la versión del RTP. En este caso la versión es 2.

- **Padding (P) - 1 bit**. Si el bit de relleno esta seteado[24], el paquete contiene uno o más octetos adicionales de relleno al final, los cuales no son parte de la multimedia. El último octeto del relleno contiene un numero que indica cuantos octetos de relleno deben ser ignorados. El relleno puede ser

[24] El valor del bit es un 1 lógico.

necesario para algunos algoritmos de encriptación con tamaños de bloques fijos o para transportar varios paquetes RTP en un protocolo de nivel inferior.

- **Extensión (X) - 1 bit**. Si el bit de extensión esta seteado, el encabezado fijo es seguido por exactamente una extensión de encabezado.

- **Contador CSRC (CC) - 4 bits**. El contador CSRC contiene el número de identificadores CSRC que siguen el encabezado fijo.

- **Marcador (M) - 1 bit.** La interpretación del marcador es definida por un perfil. Esto es propuesto para permitir eventos significativos como los límites del esquema para ser marcados en la cadena de paquetes.

- **Payload type (PT) - 7 bits**. Este campo identifica el formato de Multimedia RTP y determina su interpretación por parte de la aplicación. Un perfil especifica un mapeo estático por defecto de los códigos de los tipos de multimedia a los formatos multimedia.

- **Sequence number - 16 bits**. El número de secuencia incrementa en uno por cada paquete de datos RTP enviado, y puede ser usado por el receptor para detectar paquetes perdidos y para restaurar la secuencia de ellos. El valor inicial de los números de secuencia es aleatorio (Impredecible) para hacer el reconocimiento de texto plano y la encriptación mas difícil, incluso si la fuente por si misma no encripta, ya que los paquetes pueden fluir hacia el traductor que lo hace por esta.

- **Timestamp - 32 bits**. La marca de tiempo refleja el instante de muestreo del primer octeto del paquete de datos RTP. El instante de muestreo debe ser tomado de un reloj que se incrementa linealmente en el tiempo para permitir la sincronización y el cálculo de los Jitter[25]. La resolución del reloj debe ser suficiente para la exactitud de sincronización deseada. La frecuencia del reloj depende del formato de los datos transportados como multimedia y es especificado estáticamente en el perfil o la especificación del formato de multimedia, o debe ser especificada dinámicamente si es necesario. El valor inicial de la marca de tiempo es aleatorio, tal como el número de secuencia. Varios paquetes RTP consecutivos pueden tener igual marca de tiempo si estos son generados como una sola parte.

- **SSRC - 32 bits**. El campo SSRC identifica la fuente de sincronización. Este identificador es escogido aleatoriamente con el propósito de que dos fuentes de sincronización no vayan a tomar el mismo numero de identificador SSCR. La probabilidad de que se escojan identificadores SSCR iguales es muy baja; de todos modos todas las implementaciones de RTP están preparadas para resolver colisiones.

- **CSRC list - 0 a 15 items, 32 bits cada uno**. La lista CSRC identifica las fuentes contribuyentes para la multimedia contenida en el paquete. El número de identificadores es dado por el campo CC. Si hay más de 15 fuentes contribuyentes, solo 15 pueden ser identificadas. Los identificadores son insertados por mezcladores, usando los identificadores SSRC de las fuentes contribuyentes.

[25] Se refiere al nivel de variación de retado en la entrega de datos que introduce una red.

5. 3 RTCP (PROTOCOLO DE CONTROL RTP)

5. 3. 1 Introducción. El protocolo RTP de control (RTCP) esta basado en una transmisión periódica de paquetes de control a todos los participantes en la sesión usando el mismo mecanismo de distribución que el de paquetes de datos. El protocolo inferior debe proveer multiplexación de los paquetes de datos y de control, por ejemplo usando números de puertos separados con UDP. El RTCP desarrolla 4 funciones.

- La primera función es proveer retroalimentación de la calidad de distribución de datos. Esta es una parte integral del papel del RTP como protocolo de transporte y esta relacionado con el control de flujo y congestión de otros protocolos de transporte. La realimentación puede ser directamente útil para el control de codificadores adaptativos. Enviar reportes de realimentación de la recepción a todos los participantes permite, a quien esta observando problemas, evaluar si son locales o globales. Es posible también enviar reportes a un posible proveedor de Internet o administrador de red para que actúe como tercero para monitorear y diagnosticar posibles problemas en la red.

- El RTCP lleva un identificador persistente de Nivel de Transporte para una fuente RTP llamado nombre canónico o CNAME. Puesto que el identificador SSRC puede cambiar si es descubierto un conflicto o un programa es reiniciado, los receptores requieren el CNAME para seguir la pista de cada participante. Los receptores además requieren el CNAME para asociar múltiples flujos de datos de un participante dado en un juego de sesiones RTP relacionadas, por ejemplo para sincronizar Audio y Video.

- Las primeras dos funciones requieren que todos los participantes envíen paquetes RTCP, por esto la tasa debe ser controlada por el RTP para manejar un gran numero de participantes. Como cada participante recibe los paquetes de control de todos los demás, este puede calcular el número de ellos en la sesión presente y utilizar ese número para calcular la tasa a la cual los paquetes son enviados.

- La cuarta función es opcional, y su propósito es convenir una mínima información de control, por ejemplo la identificación de participante a ser mostrada en la interfase de usuario.

5. 3. 2 Formato del paquete RTCP. A continuación se definen varios tipos de paquetes RTCP que llevan una variedad de información de control.

- **SR Sender report**. Reporte del emisor, para estadísticas de transmisión y recepción de los participantes que son emisores activos.

- **RR Receiver report**. Reporte del receptor, para estadísticas de recepción de participantes que no son emisores activos.

- **SDES Source description ítems**. Ítems de descripción de la fuente, este incluye el CNAME.

- **BYE**. Indica el fin de la participación.

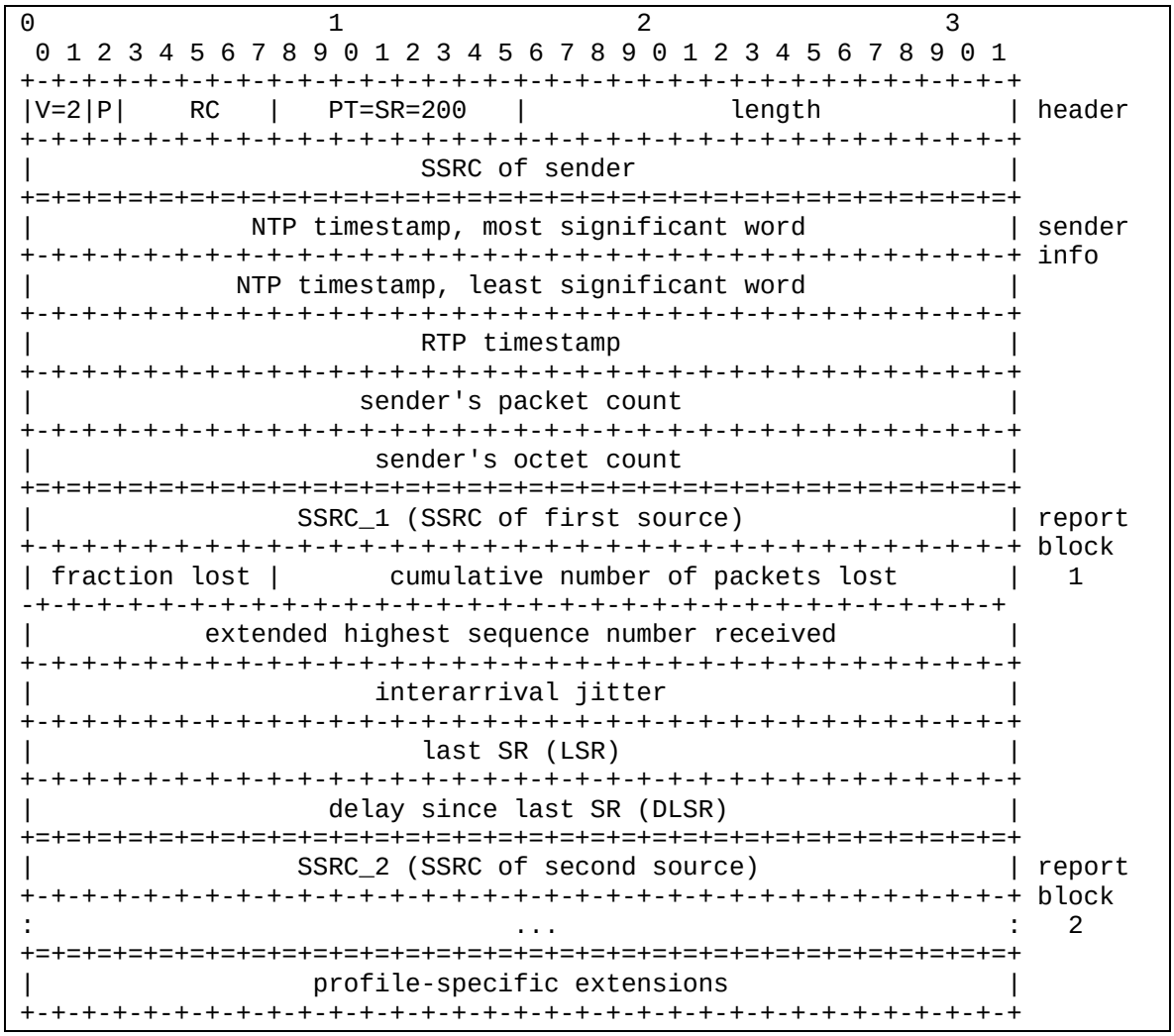
- **APP**. Funciones especificas de la aplicación.

Cada paquete RTCP comienza con una parte fija similar a los paquetes RTP, seguida de una estructura de elementos que pueden ser de longitud variable de acuerdo con el tipo de paquete pero siempre finaliza en el límite de 32 bits. El requerimiento de alineación y un campo de longitud en la parte fija son incluidos para hacer los paquetes RTCP apilables. Múltiples paquetes pueden ser concatenados, sin necesidad de separadores, para formar un paquete RTCP compacto que es enviado en un simple paquete de un protocolo de una capa mas baja, por ejemplo UDP.

5. 3. 3 Reportes de envío y recepción. Los receptores de RTP proveen realimentación de la calidad de la recepción usando los paquetes de reportes del RTCP los cuales pueden ser de dos formas dependiendo de si estos son o no emisores activos. La única diferencia entre los reportes de transmisión (SR) y los de Recepción (RR), además del código de tipo de paquete, es que el reporte de transmisión tiene una sección adicional de 20 Bytes para uso de los emisores activos.

Ambos reportes incluyen cero o mas bloques de reportes de recepción, uno por cada una de las fuentes de las cuales el receptor recibió paquetes RTP desde el último reporte. Los reportes no fueron hechos para fuentes contribuyentes listadas en la lista de CSRC. Un máximo de 31 bloques de reportes de recepción puede ir en un paquete SR o RR, los adicionales deben comenzar a apilarse para ser enviados en el siguiente reporte.

Figura 8. Formato de reporte del emisor



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

El paquete de reporte del emisor consiste en tres secciones, seguidas posiblemente de una cuarta parte de extensión específica de algún perfil si es definida. En la primera sección, el encabezado es de 8 octetos. Los campos tienen el siguiente significado.

- **Versión (V) - 2 bits**. Identifica la versión del RTP, la cual es la misma para los paquetes RTCP.

- **Padding (P) - 1 bit**. Si el bit de relleno esta seteado, el paquete contiene uno o más octetos adicionales de relleno al final, los cuales no son parte de la multimedia. El último octeto del relleno contiene un número que indica cuantos octetos de relleno deben ser ignorados. El relleno puede ser necesario para algunos algoritmos de encriptación con tamaños de bloques fijos o para transportar varios paquetes RTP en un protocolo de nivel inferior.

- **Reception report count (RC) - 5 bits**. Es el número de bloques de reportes de recepción contenidos en el paquete. Un valor de cero es valido.

- **Packet type (PT) - 8 bits**. Contiene la constante 200 para identificar este como un paquete SR de RTCP.

- **Length - 16 bits**. La longitud de este paquete RTCP en palabras de 32 bits menos uno. Incluyendo el encabezado y algo de relleno.

- **SSRC - 32 bits**. El identificador de fuente de sincronización para quien origino este paquete SR.

La segunda sección contiene la información del emisor, es de 20 octetos de largo y se presenta en todos los paquetes de reportes del emisor. Los campos tienen el siguiente significado.

- **NTP timestamp - 64 bits**. Es la Marca de Tiempo. Indica el tiempo en que el reporte fue enviado y se debe usar en combinación con las marcas de tiempo retornadas en los reportes de recepción para que los otros receptores puedan medir el tiempo de ida y vuelta para cada receptor.

- **RTP timestamp - 32 bits**. Corresponde al mismo tiempo del NTP Timestamp, pero en las mismas unidades y con el mismo Offset aleatorio que los Timestamp RTP en sus paquetes de datos.

- **Sender's packet count - 32 bits**. El número total de paquetes de datos RTP transmitidos por el emisor desde el comienzo de la transmisión hasta el momento en que el paquete SR fue generado. Este contador se resetea si el emisor cambia su identificador SSRC.

- **Sender's octet count - 32 bits.** Es el número total de octetos de los datos multimedia, es decir, sin contar con el encabezado y el relleno, transmitidos en los paquetes de datos RTP por el emisor desde el comienzo de la transmisión hasta el momento en que el paquete SR fue generado.

La tercera sección contiene cero o más bloques de reportes de recepción dependiendo del número de fuentes escuchadas por este emisor desde el último reporte. Los campos de esta sección se describen a continuación.

- **SSRC_n (source identifier) - 32 bits**. El identificador SSRC de la fuente a la cual pertenece la información del reporte de recepción.

- **Fraction lost - 8 bits**. La fracción de paquetes RTP perdidos de una fuente N desde el reporte SR o RR previamente enviado.

- **Cumulative number of packets lost - 24 bits**. El numero total de paquetes perdidos de la fuente N desde el inicio de la recepción. Es la resta de los paquetes esperados menos los recibidos actualmente, incluyendo los tardíos o los duplicados.

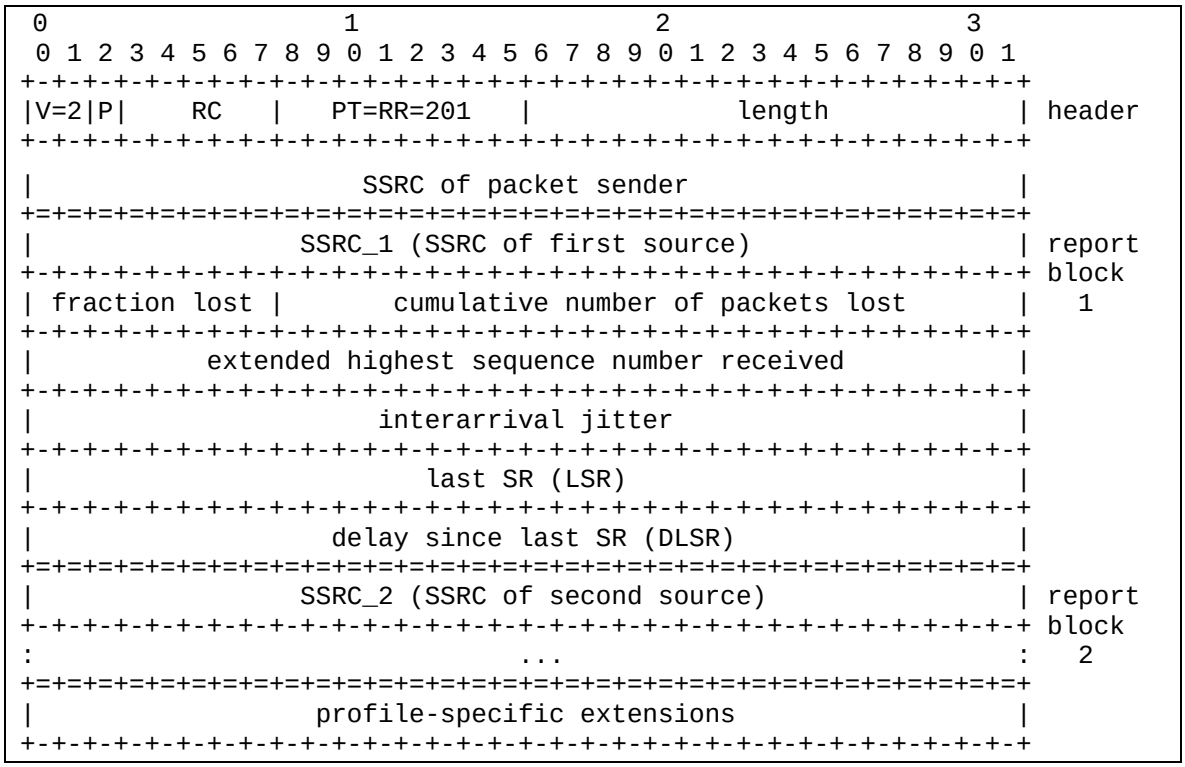
- **Interarrival jitter - 32 bits**. Es un estimado de la varianza estadística del intervalo de llegada del paquete RTP, medido en unidades de tiempo y expresado como un número entero sin signo. Este factor es definido para ser la desviación promedio de la diferencia en el espaciado de los paquetes en el receptor comparado con la fuente para un par de paquetes.

- **Last SR timestamp (LSR) - 32 bits**. Los 32 bits de la primera mitad de los 64 bits del campo NTP timestamp recibidos como parte del paquete de reporte de emisor RTCP mas reciente de la fuente N. Si no se ha recibido ninguno todavía, el campo se pone en cero.

- **Delay since last SR (DLSR) - 32 bits**. El retardo, expresado en unidades de 1/65536 segundos, entre la recepción del último paquete SR de la fuente SSRC-N y el envío del reporte de Recepción. Si no se ha recibido ningún reporte todavía entonces este campo se pone en cero.

El formato de paquete de reporte de recepción (RR) es el mismo que el del paquete SR excepto que el campo de Tipo de paquete (Packet Type) contiene la constante 201 y las cinco palabras de 32 bits de la información del emisor son omitidas. (Estas son NTP y RTP Timestamps, Senders's packet y Octet counts).

Figura 9. RR: Paquete de reporte de receptor RTCP



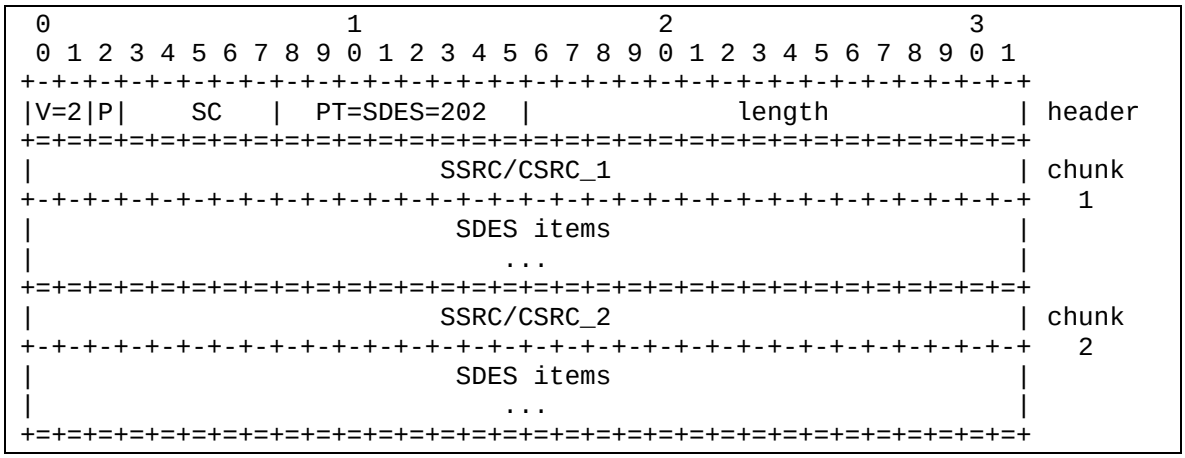
Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

5. 3. 4 Control de paquetes de reporte. En transmisiones multicast la información de control puede consumir un ancho de banda considerable (2 o 3 personas en audio conferencia consumen cierta cantidad de ancho de banda

para información de control, ¿cuánto se consumirá con 1000 personas?). Para manejar este problema RTCP ha establecido un mecanismo para reducir la transmisión de información de control a medida que ingresan más nodos a la conferencia. El mecanismo es complejo para explicarlo en este documento, pero la meta básica es limitar la cantidad de tráfico de RTCP a un pequeño porcentaje del tráfico de datos en RTP (normalmente el 5%). También es recomendado asignar más ancho de banda RTCP a los emisores activos, bajo el supuesto que la mayoría de los participantes desean ver los reportes enviados por ellos, como por ejemplo saber "quién habla".

5. 3. 5 SDES. Paquete RTCP de descripción de fuente

Figura 10. Formato del SDES



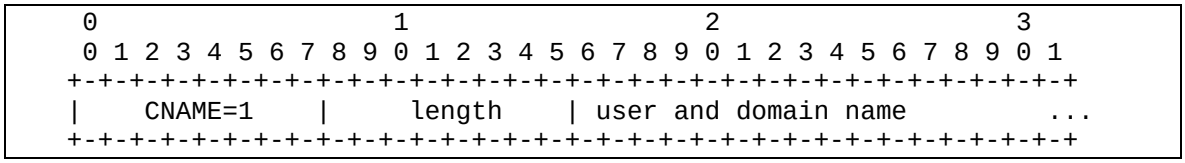
Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

El paquete SDES es un estructura de tres niveles compuesta por un encabezado y cero o mas pedazos, cada uno de los cuales esta compuesto de

ítems que describen la fuente identificada en el bloque. Cada pedazo del bloque consiste de un identificador SSRC/CSRC seguido de una lista de ítems. Cada ítem consiste en un campo de tipo de 8 bits, un contador de 8 bits que describe la longitud del texto y el texto mismo. A continuación se describen los ítems que pueden encontrarse en el paquete SDES.

- **CNAME (identificador canónico)**. Nombre canónico de la fuente de sincronismo.

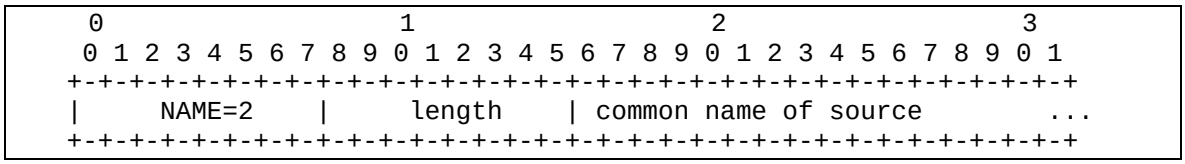
Figura 11. Formato del campo CNAME



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

- **NAME**. Nombre de usuario.

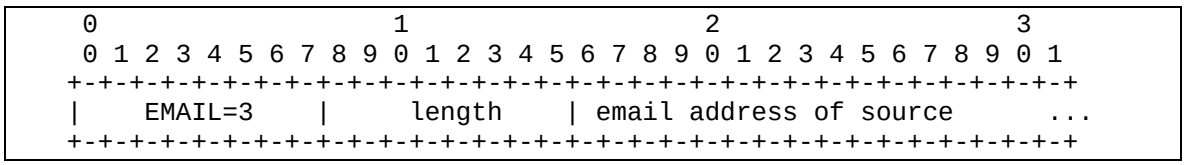
Figura 12. Formato del campo NAME



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

❖ **EMAIL**. Correo electrónico.

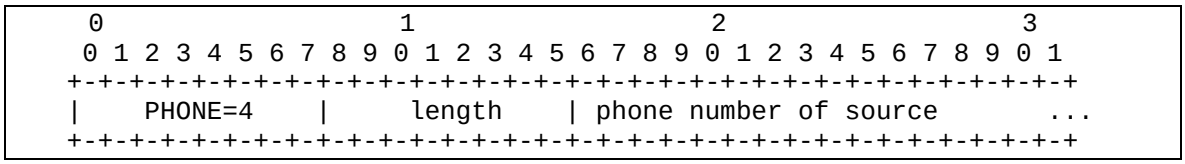
Figura 13. Formato del campo EMAIL



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

❖ **PHONE**. Número telefónico. El número telefónico debe tener el siguiente formato, reemplazando el + por el código de acceso internacional: "+1 908 555 1212".

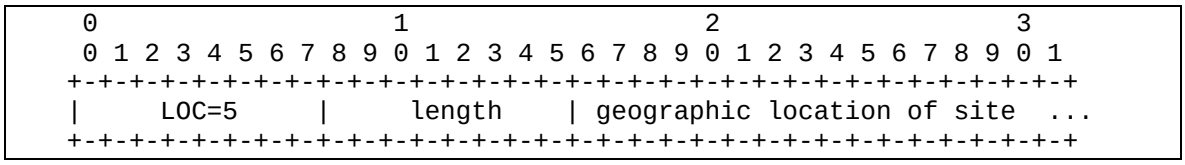
Figura 14. Formato del campo PHONE



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

❖ **LOC**. Ubicación geográfica del usuario. Es para cuestiones de información y puede ser útil a nivel administrativo para determinar posibles fallas debido a la distancia y los posibles retardos que se puedan ocacionar.

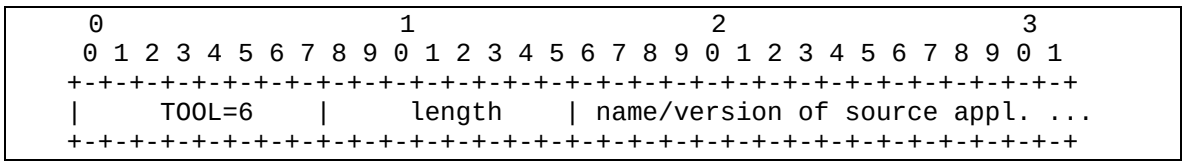
Figura 15. Formato del campo LOC



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

- **TOOL**. Nombre de aplicación o herramienta.

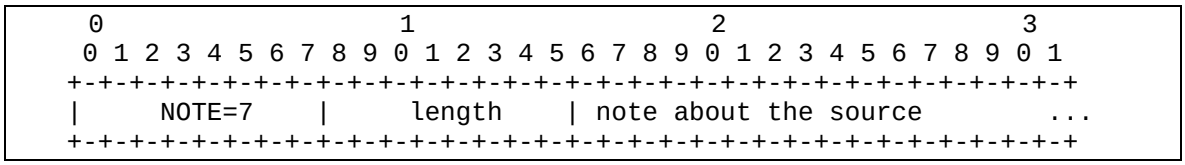
Figura 16. Formato del campo TOOL



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

- **NOTE**. Anotación o estado.

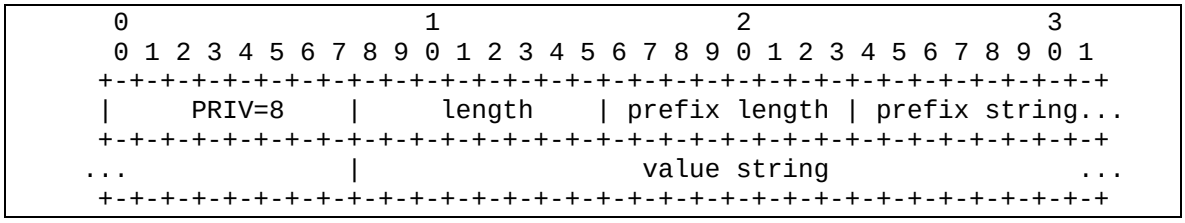
Figura 17. Formato del campo NOTE



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

❖ **PRIV**. Extensión privada. Es un campo opcional que se usa para colocar información privada del usuario.

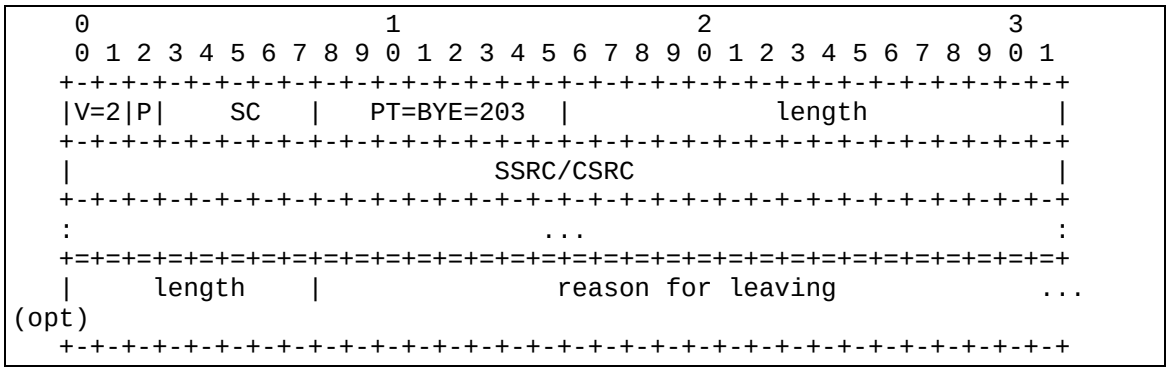
Figura 18. Formato del campo PRIV



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

5. 3. 6 BYE. Paquete RTCP de despedida. El paquete BYE indica que una o mas fuentes ya no están activas en la sesión.

Figura 19. Formato del campo BYE



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

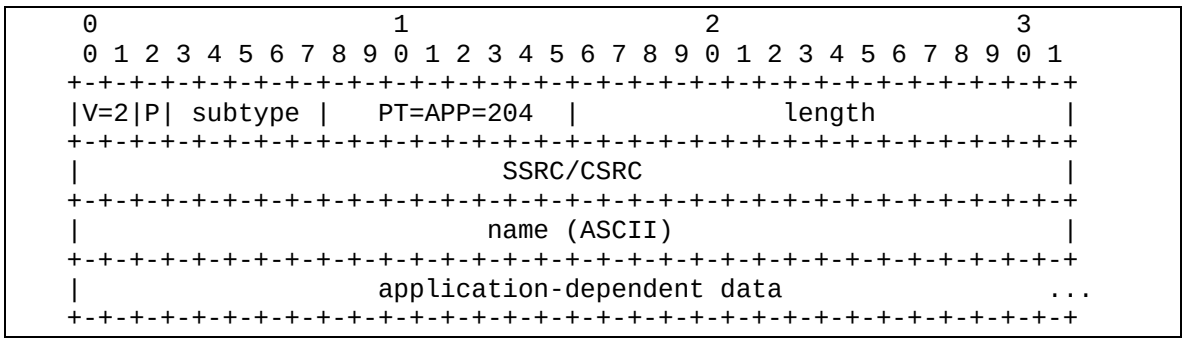
- **Packet type (PT) - 8 bits**. Contiene la constante 203 para identificar que este es un paquete RTCP BYE.

- **Source count (SC) - 5 bits**. El numero de identificadores SSRC/CSRC incluidos en este paquete BYE. Un contador en ceros es valido pero inútil.

5. 3. 7 APP. Paquete RTCP de definición de aplicación.

El paquete APP fue definido para el uso experimental de nuevas aplicaciones y nuevas características que están en desarrollo, sin necesidad de tener un registro específico del nombre de tipo de paquete. Los paquetes APP sin nombre reconocido serán ignorados.

Figura 20. Formato del paquete APP



Fuente: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

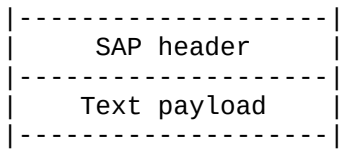
5. 4 SDP (PROTOCOLO DE DESCRIPCIÓN DE SESIÓN)

5. 4. 1 Introducción. En la infraestructura del Internet multicast, una herramienta de descripción de sesión es usada para anunciar conferencias multimedia, para informar la dirección del equipo a entrar en la conferencia y para especificar la herramienta a ser usada.

5. 4. 2 Uso del SDP.

- **Anuncios multicast**. El SDP es el Protocolo de Descripción de Sesión para sesiones multimedia. Es usado comúnmente cuando un cliente desea anunciar una sesión de conferencia enviando periódicamente un paquete de anuncio multicast a puertos y direcciones multicast bien conocidas usando el Protocolo de Anuncio de Sesión (SAP).

  Los paquetes SAP son paquetes UDP con el siguiente formato:



  El texto debe ser menor que un Kilobyte [26]de longitud. Si se anuncia por medio de SAP, solo un anuncio de sesión es permitido en un único paquete.

- **Correo electrónico y anuncios www**. Una forma de transportar descripciones de sesión son el correo electrónico y el World Wide Web (WWW). Para ambas debe ser usado el tipo de contenido

[26] 1024 Bytes

MIME[27] *"Aplicación/SDP".* Esto habilita la carga automática de aplicaciones para participación en la sesión desde el Cliente WWW o el lector de correo en una manera estándar. Nótese que los anuncios de sesiones multicast hechos vía correo electrónico o vía WWW no tienen la propiedad de ser necesariamente recibidos por el destinatario del anuncio de sesión, ya que las sesiones multicast están restringidas en alcance y libertad, y el acceso al servidor WWW o la recepción de correo esta posiblemente fuera de alcance para el.

5. 4. 3 Requerimientos y recomendaciones. El propósito del SDP es transmitir información acerca de los flujos de media en sesiones multimedia para permitir a los receptores de una descripción de sesión participar en ella. SDP es principalmente propuesto para uso en el InternetWork, aunque este es lo suficientemente general que puede describir conferencias en otros ambientes y tipos de redes. Una sesión multimedia, para estos propósitos, es definida como un juego de flujos media que están por un tiempo determinado. Los flujos de media pueden ser de varios a varios usuarios.

Hasta aquí, las sesiones basadas en multicast en el Internet han diferido de otras formas de conferencia en que cualquiera que recibe el trafico puede entrar en la sesión (a menos que el trafico este encriptado[28]). En estos ambientes multicast, SDP sirve para dos propósitos: uno para comunicar la existencia de una sesión y la otra es transmitir suficiente información para habilitar el ingreso y participación de los usuarios en la sesión. En un ambiente unicast, solamente el segundo propósito es relevante. El protocolo SDP incluye:

[27] Sistema que permite integrar dentro de un mensaje de correo electrónico ficheros binarios.
[28] Enmascarar información con signos normales que solo tienen sentido a la luz de una clave secreta.

- Nombre y propósito de la sesión.
- Tiempo(s) en que la sesión esta activa.
- La Media comprendida en la sesión.
- La información para recibir estos Media (Direcciones, puertos, formatos y algunas mas).

Como los recursos necesarios para participar en una sesión pueden ser limitados, alguna información adicional puede ser deseable:

- Información sobre el ancho de banda a ser usado en la sesión.
- información del contacto para la persona responsable por la sesión.

En general, El SDP debe transportar suficiente información para ser capaz de establecer una sesión (Con la posible omisión de claves de encriptación) y para anunciar los recursos a ser usados por los participantes que aun no hacen parte de la sesión y que posiblemente necesitan conocer los que ya hacen parte de ella.

- **Información Multimedia**. El SDP incluye:
  - El tipo de Media (Video, audio, etc.).
  - El protocolo de transporte (RTP/UDP/IP,H.320, etc).
  - El formato de la Media (H.261 video, MPEG video, oct).

  Para sesiones IP Multicast, la siguiente información debe ser enviada.
  - Dirección Multicast para Media.
  - Puerto de transporte para la Media.

Para sesiones IP Unicast, la siguiente información debe ser enviada.

- Dirección remota para Media.
- Puerto de transporte para dirección del contacto.

La semántica de esta dirección y puerto depende de la Media y protocolo de transporte definido. Por defecto, este es la dirección y puerto remoto a la cual los datos son enviados, y la dirección remota y el puerto local en el cual los datos son recibidos. También se puede usar esto para establecer un canal de control del actual flujo de Media.

- **Información de tiempo**. Las sesiones pueden ser limitadas o ilimitadas en tiempo. Ya sean o no limitadas, estas pueden ser activadas solo en tiempos específicos.

- **Sesiones Privadas**. Es posible crear sesiones públicas y privadas. Las privadas típicamente son transmitidas encriptando la descripción de la sesión. Si un anuncio de sesión es privado es posible usar este anuncio para transmitir llaves de cifrado necesarias para la de decodificación de los paquetes de datos multimedia en la conferencia, incluyendo suficiente información para saber cual esquema de encriptación es usado para cada Media.

- **Obtención de información adicional acerca de una sesión**. Una descripción de sesión debe transmitir suficiente información para decidir ya sea su participación o la exclusión en una sesión específica. SDP puede incluir puntos adicionales en la forma de Universal Resources Identifiers (URIs) para más información sobre la sesión.

- **Categorización**. Cuando varias descripciones de sesión están siendo distribuidas por SAP o algún otro mecanismo de avisos, puede ser deseable filtrar los anuncios de interés de los que no lo son. SDP soporta un mecanismo de categorización para sesiones el cual puede ser automatizado.

- **Internacionalización**. La especificación SDP recomienda usar el "ISO 10646 Character Sets" (juego de caracteres) en el codificador UTF-8 [29](RFC 2044) para permitir que varios lenguajes sean identificados. La internacionalización solo aplica para campos de "Texto Libre" (Nombre se sesión e información de respaldo).

5. 4. 4 Especificación SDP. Las Descripciones de sesión son enteramente textuales y usan el juego de caracteres ISO 10646 en codificación UTF-8. Los campos de nombre y atributos de nombre usan solo el subgrupo US-ASCII del UTF-8, pero los campos textuales y los valores de atributos pueden usar el juego completo de caracteres ISO 10646. La forma textual fue elegida para ampliar la portabilidad, para habilitar la variedad de transportes a ser usados y para permitir la flexibilidad del juego de herramientas, basadas en texto (Tcl/Tk), a ser usadas para generar y procesar descripciones de sesión. No obstante, como el ancho de banda otorgado para todos los anuncios SAP es estrictamente limitado, la codificación es bastante compacta. Además, puesto que los anuncios pueden ser transportados por medios poco confiables o dañados por servidores de manipulación intermedia, la codificación fue diseñada con estrictas reglas de orden y formato. Por esta razón, la mayoría de los errores en los anuncios malformados pueden ser detectados y descartados rápidamente. Esto también permite descartar anuncios para los cuales los receptores no tienen las llaves válidas de encriptación.

[29] Es un mecanismo estándar usado por Unicode para codificar valores de caracteres amplios en una secuencia de bytes.

Una descripción de sesión SDP consiste en un conjunto de líneas de texto de la forma <Tipo>=<Valor>. <Tipo> siempre es exactamente un carácter y es sensible a mayúsculas. <Valor> es una cadena de texto estructurada cuyo formato depende del <Tipo>. Este será además sensible a la mayúscula a menos que un campo especifico defina lo contrario. Los espacios en blanco no se permiten en ambos lados del signo '='.

Un anuncio consiste en una sección de *Nivel de Sesión* seguido de cero o más secciones de *Nivel de Media.* La sección de Nivel de Sesión comienza con una línea "v=" y la sección de Nivel de Media comienza con una línea "m=".

Cuando SDP se transmite vía SAP solo una descripción de sesión se permite por paquete. Cuando es por otros métodos, varias descripciones de sesión pueden ser concatenadas una tras otra en el mismo orden que se mostrara a continuación. No todas las líneas de descripción son requeridas, pero si aparecen deberán hacerlo en este orden. Los ítems adicionales se marcan con un '*'.

- Descripción de Sesión.
  - v= (Versión del Protocolo)
  - o= (Creador e identificador de Sesión).
  - s= (Nombre de Sesión)
  - i=* (Información de la Sesión)
  - u=* (URI de descripción)
  - e=* (Dirección de correo electrónico)
  - p=* (Numero Telefónico)
  - c=* (Información de Conexión)
  - b=* (Información del Ancho de Banda)

- z=* (Ajustes de Zona Horaria)
- k=* (Clave de Encriptación)
- a=* (Cero o mas líneas de atributos de Sesión)

❖ Descripción de Tiempo.
- t= (Tiempo que la sesión esta activa)
- r=* (Cero o mas repeat times)

❖ Descripción de Media.
- m= (Nombre del Media y dirección de transporte)
- i=* (Titulo de Media)
- c=* (Información de conexión)
- b=* (Información de Ancho de Banda)
- k=* (Clave de Encriptación)
- a=* (Cero o mas líneas de atributos de Media)

El juego de letras de 'Tipos' es deliberadamente pequeño y propuesto para ser extensible. Todas las letras de tipos que no se entiendan serán ignoradas en el SDP. La información de conexión ('c=') y el atributo ('a=') en la sección de Nivel de Sesión aplica para todos los tipos de Media de esa sesión, a menos que sean anulados por la existencia de alguno de estos parámetros con el mismo nombre en la descripción de Media. Un ejemplo de una Descripción SDP es el de la figura 21.

Los textos grabados como el nombre de sesión y la información son cadenas de Bytes que pueden contener cualquier valor excepto 0x00 (Null), 0x0a (ASCII nueva línea) y 0x0d (ASCII retorno de carro). La secuencia CRLF

(0x0d0a) es usada para terminar un registro, aunque los analizadores deben ser un poco tolerantes y deben permitir que algunos registros terminen con un simple final de línea. La descripción de cada uno de los campos se hace a continuación.

Figura 21. Ejemplo descripción de sesión

```
v=0
o=shi_papp 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminario
i=Un Seminario del Protocolo SDP
u=http://www.ipsofactum.com
e=shi_papp@hotmail.com (Andres Botero)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

- **Versión del Protocolo - v=0**. Este campo contiene la versión de Protocolo SDP.

- **Origin**. o=<username><session id><version><network type> <address type><address>. Este campo entrega el agente que origina de la sesión (El Username y la dirección del equipo del usuario) mas un identificador de Sesión y un numero de versión de sesión. A continuación se describen cada uno de los subcampos del origen.

  - **Username**. Es el Login del usuario en el equipo de origen, o es "-" si este no soporta el concepto de ID de usuario. El Login no debe contener espacios.

- **Session id**. Es una cadena de números tal que el grupo de <username>, <session id>, <network type>, <address type> y <address> forman un identificador globalmente único para la sesión. El método de ubicación por <Sesión ID> es suficiente, pero fue sugerida una estampa de tiempo del Protocolo de tiempo de Red (NTP) con el fin de asegurar la unicidad de las sesiones.

- **Versión**. Es el número de versión para este anuncio. Esto es necesario para que los servidores Proxy detecten cual de los varios anuncios para la misma sesión es el más reciente.

- **Network type**. Es una cadena de texto con el tipo de Red. Inicialmente "IN" denota que es Internet.

- **Address type**. Es una cadena de texto con el tipo de dirección. Inicialmente se han definido IPv4 e IPv6. Para cualquiera de los dos, este campo de dirección debe ser el dominio completo de la maquina que crea la sesión. Si no se tiene registrado un dominio valido entonces se debe poner la notación decimal de la dirección en caso de que sea IP4; Si es IP6 la representación textual comprimida. No se deben usar direcciones inválidas dentro de redes ya que están fuera del alcance de cualquier equipo por fuera de ella.

- **Session Name**. s=<session name>. Es el nombre de la sesión. Debe haber un solo nombre de sesión por cada paquete de Descripción de Sesión, además debe contener el juego de caracteres ISO 10646.

- **Información de la Sesión y del Media**. i=<session description>. No debe haber más de un campo de información en la descripción. Si la existe debe ser una cadena de texto. Es mas comúnmente usado para etiquetar los tipos de flujos de media en la sesión.

- **URI**. u=<URI>. Universal Resource Identifier (identificador de recursos universal) usado por clientes WWW. Es opcional y debe ser especificado antes del primer campo de Media. No puede haber más de un URI por Descripción.

- **Email Address and Phone Number**. e=<email address>, p=<phone number>. Son información adicional del contacto. Si existen deben estar antes del primer campo de media. Puede haber más de un correo o teléfono.

- **Connection Data**. c=<network type><address type><connection address>. Puede haber un campo de estos en el nivel de sesión y otro en el nivel de media. El primer subcampo es el tipo de red, inicialmente definido como 'IN' parea denotar Internet. El segundo es el tipo de dirección; Solamente se ha definido el IPv4. El tercer subcampo es la dirección de conexión. Otros subcampos adicionales se pueden incluir dependiendo del valor de <Address type>. A continuación se muestra un ejemplo.

c=IN IP4 224.2.1.1/127/3
<Network Type>/<Address Type>/<base multicast address>/<ttl>/<number of addresses>

- **Bandwidth**. b=<modifier>:<bandwidth-value>. Especifica el ancho de banda propuesto para ser usado por la sesión o la Media y es opcional.

  - **<Bandwidth-value>**. Es el ancho de banda disponible para el canal y se expresan **kilobits** por segundo (kbps).

  - **<Modifier>**. Es una palabra alfanumérica como de la siguiente forma.

    b=X-YZ:128

- **Encryption Keys**. Son las llaves de encriptación que se utilizan para cifrar la información como una medida de seguridad. Este campo tiene el siguiente formato:

  k=<method>:<encryption key>. El SDP puede ser usado para mandar ***Llaves de Encriptación***. Si se pone antes del primer campo de media aplica para todos estos. El método indica el mecanismo a ser usado. Los siguientes métodos están definidos:

  - **k=clear:<encryption key>**. La clave de encriptación se incluye sin ninguna transformación.

- **k=base64:<encoded encryption key>**. La clave de encriptación es incluida en este campo pero ha sido codificada en Base64 porque esta incluye caracteres que son prohibidos en SDP

- **k=uri:<URI para obtener la llave>**. Un URI es incluido en este campo. El URI se refiere a los datos que contienen llave de encriptación, y puede requerir autenticación adicional antes de que esta pueda ser retornada.

- **k=prompt**. No se incluye ninguna llave en esta descripción, pero la sesión o el flujo de media referida por este *Campo de Llave* esta encriptado.

- **Media Announcements**. m=<media><port><transport><fmt list>. Una descripción de sesión puede contener un número de descripciones de Media. Cada una de estas empieza con un campo "m=", y es terminado por el comienzo de otro de estos o el fin de la descripción de la sesión. Un campo de media además tiene varios subcampos:
  El primero es el tipo de media. Corrientemente los tipos definidos son *Audio, Video, Aplicación, Datos, Control.* Otros tipos irán apareciendo en el futuro. El segundo es el puerto de transporte por el cual el flujo de media va a ser enviado. Para transporte basado en UDP, el valor debe ser en el rango de 1024 a 65535. Para RTP el puerto debe ser un número par. Para aplicaciones donde se codifican los flujos que se envían a direcciones unicast, puede ser necesario especificar múltiples puertos de transporte. Esto se hace usando una notación similar a la usada para direcciones Multicast en el campo "c=". El formato seria el siguiente.

m=video 49170/2 RTP/AVP 31

m=<media> <port>/<number of ports> <transport> <fmt list>

Lo cual especifica que los puertos 49170 y 49171 para un par RTP/RTCP y el 49172 y 49173 forman el segundo par RTP/RTCP. RTP/AVP es el protocolo de transporte y 31 es el formato. El tercer subcampo es el protocolo de transporte. Este valor depende del campo de tipo de dirección en el campo "c=". Para IP4 se especifica normalmente que el tráfico de media es llevado en RTP sobre UDP. Los siguientes protocolos están definidos:

- **RTP/AVP.** Es el Protocolo de Transporte en Tiempo Real de la IETF usando el perfil Audio/Video llevado sobre UDP.

- **UDP.** Protocolo de Datagramas de Usuario.

5. 5 DIFERENCIAS ENTRE INTERNET Y LA PSTN

Hay diferencias muy significativas entre Internet y la Red Telefónica Publica Conmutada (PSTN), siendo la más importante, la diferente técnica de conmutación que utilizan paquetes y circuitos, respectivamente. Otra diferencia significativa es que Internet usa un enrutamiento dinámico basado en una dirección no geográfica, mientras que en la PSTN el direccionamiento es estático y basado en una numeración asociada a una localización geográfica: el número telefónico. Por otro lado, Internet tiene una arquitectura

descentralizada, lo que resulta en una mayor flexibilidad y permite un despliegue más rápido de las aplicaciones.

Un aspecto muy importante a destacar, que no tiene que ver con los técnicos, es la diferente regulación que afecta a una y otra red. Mientras que la PSTN ha estado y sigue sujeta a una extensa regulación en todos los países que inhibe la competencia real, Internet es una red abierta lo cual la favorece y promueve para facilitar la entrada en nuevos mercados.

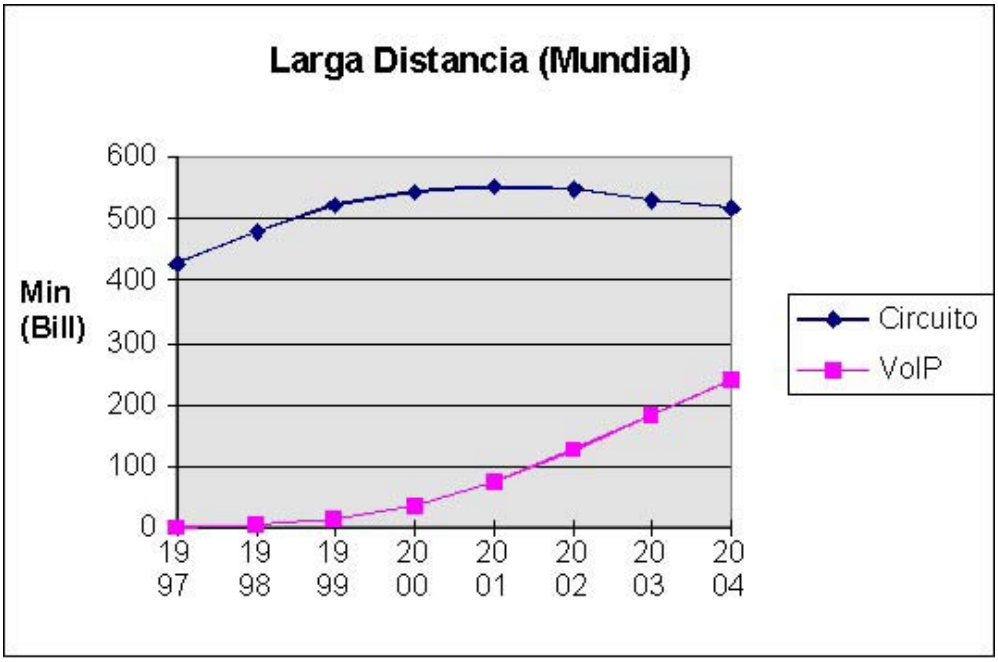
Por otra parte, en muchos países las tarifas del servicio telefónico no se corresponden con los costos del mismo, lo que hace que resulten excesivamente altas, sobre todo para las llamadas internacionales. Esta situación crea una gran oportunidad para los servicios de voz sobre IP a través de Internet, al ser su costo muy inferior ya que no depende de la distancia y se aplica tarifa local. También se puede utilizar una red IP privada constituida a tal efecto.

Dado que Internet se soporta sobre una nueva infraestructura de red (no se basa en la red telefónica aunque hace cierto uso de parte de ella y la mayoría de los usuarios la acceden a través de ella), obliga a recalcular los costos del servicio, establecer una nueva manera de tarifación acorde con los mismos, e implantar una regulación adecuada a la nueva modalidad; estos factores son de una importancia estratégica ya que rompen los moldes tradicionales sobre los que se han basado los monopolios de los operadores. Una infraestructura basada en routers[30] y gateways en la que la inteligencia se deja del lado de los terminales (PCs) es mucho más barata y económica de implantar y mantener -

[30] Enrutador. Dispositivo hardware o software que distribuye tráfico entre redes.

al menos en un factor de 1 a 10- que la tradicional red de conmutación telefónica en la que los terminales (teléfonos) son tantos.

Figura 22. Relación de llamadas larga distancia



Fuente: La telefonía sobre IP [en línea]. Madrid : José Manuel Huidobro, 2003. [Citado 5 de abr, 2004]. Disponible por internet : http://www.monografias.com/ trabajos10/tele/tele.shtml.

Internet se concibió como una red telefónica para interconectar ordenadores, pero puede que en el futuro sea una red de ordenadores para conectar teléfonos y proveer una verdadera telefonía. Esta afirmación quizá sea un poco aventurada pero se ve avalada por ciertos estudios recientes que predicen que el tráfico de voz sobre Internet puede superar al de datos en el plazo de unos pocos años. De hecho, ya el volumen de tráfico total sobre Internet supera al de voz sobre las redes telefónicas.

5. 6 GATEWAY DE VOZ SOBRE IP

El término pasarela de VoIP en ocasiones también se suele utilizar para hacer referencia a otros elementos funcionales, en tal caso se le suelen llamar pasarelas de VoIP especiales, en tanto que se posicionan entre redes IP para desarrollar determinadas funciones de mapeo, por ejemplo en la capa IP. Entidades específicas como servidores proxy de VoIP, trans-codificadores de VoIP, traductores de direcciones de red VoIP, etc., caen en esta categoría de pasarelas de VoIP.

Las pasarelas de interconexión en este contexto son básicamente dispositivos lógicos, aunque también pueden ser, y de hecho son, dispositivos físicos, como se verá posteriormente. Tienen una serie de atributos que caracterizan el volumen y tipos de servicios que pueden proveer, por ejemplo:

- Capacidad, expresa el volumen de servicio que puede brindar la pasarela, estando relacionado directamente con el número de puertos que tiene (igual al número máximo de llamadas simultáneas) y la velocidad del enlace de acceso.
- Protocolos de señalización soportados, tanto relativos a redes de VoIP como relativos a redes SCN.
- Codecs de voz utilizados.
- Algoritmos de encriptado que soporta.
- Rango de direccionamiento, que es el rango o abanico de números telefónicos que a su través se tiene acceso en la PSTN desde la red IP. En relación con la tarifación, este rango de direccionado puede o no estar fraccionado.

En general, las pasarelas de interconexión tienen que proporcionar los siguientes "mecanismos" o funciones:

- **Adaptación de señalización**. Básicamente tiene que ver con las funciones de establecimiento y terminación de las llamadas.
- **Control de los medios**. Se relaciona con la identificación, procesamiento e interpretación de eventos relacionados con el servicio, generados por usuarios o terminales.
- **Adaptación de medios**. Según requerimientos de las redes.

La pasarela o gateway de interconexión también desarrolla la función de control de medios, que se ocupa de "manejar" toda la información de control generada por el terminal. Para el caso de comunicaciones de voz, la información de control del nivel de usuario más destacada es la de los tonos multifrecuencia (DTMF) que produce un teclado telefónico convencional (por ejemplo, para interactuar con un servidor de voz). Ahora bien, dadas las características de estas señales, en el sentido que están en el rango audible pero no son señales de voz, sino tonos, es necesario prestar particular atención para su traspaso por la conexión híbrida que representa la pasarela de interconexión. Las técnicas de compresión de voz de baja velocidad introducen considerable distorsión en los tonos DTMF, provocando la recepción y su correspondiente decodificación incorrecta en los receptores. Entonces, esto requiere que las señales de audio y los tonos DTMF sean separados en la pasarela (si no lo ha sido ya en el emisor), y conducidos de forma independiente al receptor. Hay dos posibles soluciones para el transporte de los tonos DTMF:

- **Transporte "dentro de banda"**. Consiste en transportar estos tonos, digitalizados y empaquetados, con los protocolos RTP/UDP, mediante un formato de carga útil dedicado.

- **Transporte "fuera de banda"**. Conlleva a utilizar un canal de control de medios seguro (no UDP, sino TCP) para el transporte de las señales DTMF.

El transporte de los tonos DTMF "dentro de banda" se ve afectado por la falta de garantía en la entrega de paquetes que el protocolo UDP ofrece, con nefastas consecuencias para el funcionamiento del servicio en caso de pérdida de un paquete asociado a un tono DTMF. Tiene la ventaja de que los tonos permanecen sincronizados en el tiempo con respecto a la voz. En cambio, el transporte "fuera de banda" si bien gana en seguridad respecto a la entrega segura de los paquetes, pierden las señales su referencia exacta en el tiempo en relación con el flujo de voz. Esta es precisamente la solución adoptada en la Recomendación H.323, mediante el canal H.245.

5. 7 REQUERIMIENTOS DE UNA RED PARA SOPORTAR VOIP

A continuación se mencionan aspectos importantes que se deben tener en la red IP para implantar este servicio en tiempo real.

- Manejar peticiones RSVP que es un protocolo de reservación de recursos.
- El costo de servicio debe estar basado en el enrutamiento para las redes IP.
- Donde se conecta con la red pública conmutada un interruptor de telefonía IP debe soportar el protocolo del Sistema de Señalización 7 (SS7). SS7 se

usa eficazmente para fijar llamadas inalámbricas y con línea en la PSTN y para acceder a los servidores de bases de datos de la PSTN. El apoyo de SS7 en interruptores de telefonía IP representa un paso importante en la integración de las PSTN y las redes de datos IP.

- Se debe trabajar con un comprensivo grupo de estándares de telefonía (SS7, Recomendación H.323) para que los ambientes de telefonía IP, PBX/PSTN/ATM, vídeo y Gateways telefónicos puedan operar en conjunto en todas sus características.

5. 8 CALIDAD DE SERVICIO QoS

Esta función tiene primordial importancia en relación con la QoS experimentada por el usuario final. En esto influyen dos factores fundamentales:

- La calidad de la voz extremo a extremo, determinada por los sucesivos procesos de codificación – decodificación, y las pérdidas de paquetes en la red.
- La demora extremo a extremo, debido a las sucesivos procesos de codificación – decodificación, empaquetamiento y "en espera", afecta la interactividad en la conversación, y por tanto a la QoS. Las redes IP son redes del tipo best-effort y por tanto no ofrecen garantía de QoS, pero las aplicaciones de telefonía IP si necesitan algún tipo de garantía de QoS en términos de demora, jitter y pérdida de paquetes. En tal sentido existen dos mecanismos se señalización para QoS, esto es, IntServ [31]y DiffServ [32] . Ambos son "mecanismos" de cara a la red.

[31] Modelo de Calidad de Servicio en Servicios Integrados de Internet.
[32] Modelo de Calidad de Servicio en Internet basado en Servicios Diferenciados.

Por tanto, es necesario buscar QoS no solo en la red, sino también en los terminales, y en los procesos que en los mismos se desarrollan, de ahí que sea necesario también decir que la sensibilidad a la pérdida de paquetes, a las demoras y sus fluctuaciones, que experimentan los servicios de voz sobre IP, dependen en buena medida de los mecanismos implementados en los terminales.

La preparación de los medios en los terminales para ser enviados y transferidos por la red IP involucra varios procesos; digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor. Todo esto se lleva a cabo mediante un complejo procesamiento que sigue determinado algoritmo, lo cual a su vez se desarrolla en cierto intervalo de tiempo, esto implica demora de procesamiento y demora de empaquetado:

- **Demora de procesamiento**. Demora producida por la ejecución del algoritmo de codificación que entrega un flujo de bytes listos para ser empaquetados.

- **Demora de paquetización**. Es el tiempo que se requiere para formar un paquete de voz a partir de los bytes codificados.

Debe señalarse que el resultado de esta codificación – empaquetado incide directamente en la QoS, y también la forma en que se lleve a cabo. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que posibilita de cara a la red poder manejar más conexiones simultáneas, pero se incrementa la demora y la distorsión de la señales de voz. Lo contrario ocurre al aumentar la velocidad de codificación.

Otro aspecto a tener en cuenta es el compromiso entre la demora de empaquetado y la utilización del canal (relación entre bytes de información y bytes de cabecera en cada paquete de voz), es decir, la búsqueda de mayor utilización del canal conduce a mayor demora de empaquetado para cierto estándar de codificación. Claro está, según el estándar de codificación que se utilice será la demora resultante en relación con la utilización del canal, diferencias que se acentúan cuando la utilización del canal está por encima del 50 %, con un crecimiento de la demora en forma exponencial en el caso de los codecs de baja velocidad como el G.723.1. La demora de empaquetado también puede ser reducida mediante multiplexación de varias conexiones de voz en el mismo paquete IP.

A las demoras de procesamiento y empaquetado se suma también la demora que introduce el proceso de almacenamiento en los terminales, y la demora de "encolado" en la red. Todo esto da una demora extremo a extremo que percibe el usuario final en mayor o menor medida. Demoras extremo a extremo por debajo de 400 milisegundos no comprometen la interactividad en la conversación, pero ya por encima de 150 milisegundos se requiere control del eco.

Las demoras antes comentadas son resultado lógico de las características y modo de operación de las redes IP, así como también de la naturaleza de las señales de voz.

5. 9 CODECS

Un codec es un algorítmo que sirve para comprimir y descomprimir imágenes y audio de una aplicación multimedia. Estas imágenes o audio, descomprimidos, consumirían gran cantidad del ancho de banda disponible, de ahí que se necesite comprimirlos, y para ello se desarrollaron los codecs. La ventaja del codec es precisamente ayudar a disminuir el tamaño del archivo sin perder calidad. Igualmente para descomprimir un video/audio necesitamos el codec con el que fue comprimido. Esto es porque cada codec tiene su forma de comprimir, distinta en cada caso. De ahí la gran cantidad de codecs que existen, unos mejoran calidad, otros mejoran compresión, etc., pero es muy difícil encontrar dos iguales.

5. 9. 1 Codecs de audio.

- **G711**. La recomendación ITU-T G.711 define la cuantificación no uniforme de audio de tipo voz a 8 kHz y 8 bits por muestra (bit rate 64 kbps). Se ha empleado tradicionalmente en las comunicaciones telefónicas.

- **G723.1**. El G732.1 es un codec de bajo consumo de ancho de banda diseñado especialmente para aplicaciones de video conferencia. Especificado en el Standard ITU G.723.1, este codec utiliza una cuantificación multipulso de máxima cercanía de llegada (MP-MLQ) y un código algebraico de predicción lineal excitada de codificación del habla (ACELP).

  Alphamosaic ha desarrollado una altamente optimizada implementación del G723.1 con las siguientes especificaciones:

- Soporta ratas de bit de 6300 bps y 5300 bps.
- Soporta ratas de muestreo de 8 kHz y precisión de 16 bits.
- Soporta detección de actividad de voz (VAD).
- Generación de ruido de confort (CNG).

- **G.726**. El G.726 es un codec de audio el cual es usado en gran variedad de cámaras portátiles y estáticas digitales de video, además de webcams. Este codec es basado en un sistema modulador adaptativo de pulsos diferenciales para voz (ADPCM), con un sofisticado predictor y características que permiten estabilidad en el momento de presentarse errores. Es usado por teléfonos DECT entre una variedad de dispositivos, sin embargo, este codec en su naturaleza no puede a competir con los codecs modernos basados en CELP.

  Alphamosaic provee una altamente optimizada versión del G.726 con las siguientes características:

  - Soporta ratas de bit de 16Kbps, 24Kbps, 32Kbps y 40 Kbps.
  - Capacidades de prueba de bit mediante vectores de prueba ITU-T.

5. 9. 2 Codecs de video.

- **H.264**. Este codec es la culminación de un trabajo continuo entre la ITU-T y la ISO/IEC que lograron establecer combinación entre los estándares H.26x y MPEG. Este codec posee una eficiencia en codificación y alta calidad de imagen sin precedentes, gracias a la colaboración de estas dos organizaciones.

Este codec puede ser utilizado en casi todas las aplicaciones para ejecución de archivos de video y almacenamiento permitiendo disminuir los retardos y el espacio de almacenamiento. El mejoramiento de compresión con respecto al MPEG4 es casi del 50%. Las características principales de este se describen a continuación.

- Variedad de modos de compensación de movimiento.
- Precisión de compensación de movimiento de un cuarto de píxel.
- Codificación aritmética avanzada.
- Escalabilidad del codificador y decodificador.

- **H.263**. Este estándar que fue publicado por la ITU soporta compresión y codificación de video para aplicaciones de videoconferencia y de video-telefonía.

  Alphamosaic provee un codec H.263+ optimizado con un excelente desempeño y calidad de video.

- **MPEG4**. El es un estádar de la ISO/IEC desarrollado por el grupo MPEG (Moving Picture Experts Group), este comité también ha desarrollado los estándares MPEG-1 y MPEG-2. Este codec es el resultado de un esfuerzo internacional que involucró cientos de investigadores e ingenieros de todo el mundo. El MPEG-4 fue terminado en Octubre de 1998 y se convirtió en un estándar internacional a principios del año 1999. Las aplicaciones de este codec se describen a continuación.

- Televisión digital.
- Aplicaciones gráficas interactivas (contenidos sintéticos).
- Multimedia interactiva (WWW).

Alphamosaic prove un altamente optimizado MPEG-4 con un excelente rendimiento y calidad de video gracias a las características mostradas a continuación.

- Tiempo de procesamiento muy bajo.
- Perfiles de nivel visual basados en H.263.
- Bajo consumo de memoria.

5. 10 APACHE (SERVIDOR HTTP)

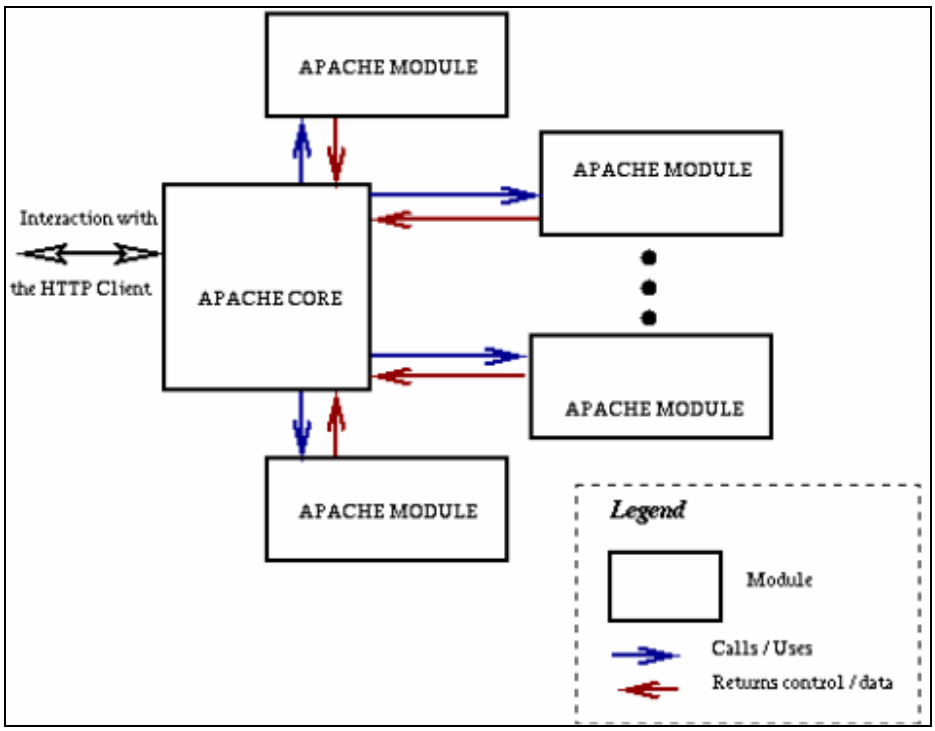
5. 10. 1 Descripción.

- **Introducción**. En el momento el Apache es el servidor web más popular en el Internet. Ha mantenido y mejorado su status desde que originalmente fue desarrollado el año 1996. La razón principal por la cual este servidor ha tenido el éxito mundialmente reconocido, es que este proyecto es completamente de código abierto. Vale la pena mencionar que este servidor fue escrito para ser completamente compatible con el servidor del NCSA.

- **Arquitectura**. La función del servidor web es la de recibir pedidos hechos a través del protocolo HTTP. Típicamente el servidor recibe pedidos de un recurso específico y retorna este recurso como respuesta. El cliente puede referenciar en su pedido un archivo, y por consiguiente el archivo es

regresado hacia el, por ejemplo, en el caso de un directorio, el contenido. Un cliente también puede hacer un pedido de un programa, y es la tarea del servidor correr el programa (CGI Script[33]) y retornar la respuesta de este al cliente. Una gran variedad de recursos pueden ser referenciados en el pedido del cliente. Para resumir, el servidor toma un pedido, lo decodifica, obtiene el recurso y se lo envía al cliente.

Figura 23. Arquitectura de APACHE



Fuente: The Conceptual Architecture of the Apache Web Server [en línea]. Waterloo, 1999. [Citado 8 de mar, 2004]. Disponible por internet : http://www.math.uwaterloo.ca/~oadragoi/CS746G/a1/apache_conceptual_arch.html.

[33] Programa de interfaz que permite al servidor de Internet ejecutar programas externos para realizar una función específica.

Algunos aspectos como el control de acceso autorizado y las autorizaciones de clientes son responsabilidad también del servidor web. Se debe asegurar que lo anterior no sea una trampa para el sistema donde corre el servidor. Además, el servidor debe estar en capacidad, no sólo de responder a una gran cantidad pedidos, sino además satisfacer estos pedidos lo más rápido posible.

- **Descripción de la arquitectura del servidor**. Al contrario de un servidor de arquitectura monolítica en el cual todas las actividades son realizadas por una sola unidad, el servidor apache toma una estructura modular cómo se muestra en la figura 23. El núcleo del servidor es la parte responsable de definir y ejecutar los pasos para dar una respuesta, controlando el paso de esta información hacia muchos módulos que actúan como fases en el procesamiento del pedido.

5. 10. 2 Instalación y configuración.

- **Prerrequisitos**.
  - Tener un computador con el sistema operativo Linux (en esta caso en particular) instalado y corriendo.
  - Poseer una conexión a Internet de mínimo 128 Kbps. Una conexión más rápida significará mejores resultados y rendimientos.
  - Se requiere tener los paquetes de instalación de Apache, Inetd y Bind 8.0 o superior. Para los anteriores se requiere que posean todas sus dependencias.

- **Configuración del servidor web Apache HTTP**. De forma predeterminada el paquete de instalación de Apache tiene como su directorio de páginas web el destino (/var/www/html/) para los sistemas

operativos RedHat 7.x, 8.x y 9.x, y para los sistemas operativos inferiores al RedHat 6.0 el destino (/home/httpd/html/). La página de inició predeterminada en la configuración es index.html. Apache puede ser configurado como servidor de un sitio web, pero también puede ser configurado para servir a múltiples dominios; lo último no será necesario en este caso.

- **Edición del archivo httpd.conf**. El archivo httpd.conf es un archivo de configuración que contiene todas las directivas, reglas y referencias a módulos para que el servidor apache se ejecute como el usuario desea. En este caso es importante tener en cuenta para la configuración tres aspectos. El primero se refiere a los módulos; se desea cargar en el archivo las dependencias correctas para qué el servidor ejecute los scripts en PHP[34]. Para lograr esto se deben adicionar las siguientes líneas en el archivo httpd.conf.

  - LoadModule php4_module
  - AddType application/x-httpd-php .php .php4

  En segundo lugar se debe referenciar el destino el cual el servidor debe tomar para encontrar los archivos relacionados con el servicio web que se desea implementar. En éste orden de ideas se debe declarar correctamente la variable DocumentRoot, sin olvidar declarar la etiqueta Directory, de la siguiente forma.

[34] Preprocesador de hipertexto.

- DocumentRoot "/var/www/html/Carpeta_que_contiene_la_Pagina_WEB"
- <Directory "/var/www/html/Carpeta_que_contiene_la_Pagina_WEB">

Por ultimo se debe referenciar el archivo que debe buscar el servidor al recibir una petición HTTP general por ejemplo www.mi_pagina.com, esto se consigue editando el archivo httpd.conf para que se pueda ejecutar esta búsqueda, de la siguiente forma.

- <IfModule mod_dir.c>
- DirectoryIndex index.php index.html
- </IfModule>

En el anterior ejemplo el servidor busca en el contenido de la ruta local declarada en la variable DocumentRoot el archivo “index.php” prioritariamente y luego el archivo “index.html” si el anterior no es encontrado en el destino.

Las herramientas anteriores permiten el desarrollo de un servicio web para complementar el servidor de telefonía de voz sobre IP que le permite a los usuarios de una forma más ágil ingresar sus datos de suscripción, de contactos, etc. y además le permite a los administradores del servicio acceder de una forma remota a las bases de datos y a la ejecución de comandos de prueba y mantenimiento del sistema.

5. 11 RECURSOS DE ÍNTERCONECTIVIDAD

5. 11. 1 ATA's (Adaptador de Teléfono Análogo). Los ATA's son un recurso de ínterconectividad muy sencillo de utilizar y configurar. En realidad el usuario solo tiene que conectar un teléfono como los que se usan para acceder a la red publica al puerto RJ11 del adaptador, y el otro a la red Ethernet (Puerto RJ45). La configuración del ATA corre por cuenta de la compañía que provee de los servicios de VoIP o por el usuario siempre y cuando cuente con los conocimientos necesarios para hacerlo.

Su función es actuar como un convertidor de una aplicación Digital (VoIP) a la señalización de los teléfonos de la red publica conmutada. Algunos de los parámetros de configuración más importantes son.

- El *password*, el cual se debe ingresar para poder acceder a la página de configuración.
- Elegir entre asignación dinámica o estática de la *dirección IP*. Si se escoge dinámica entonces se hace automáticamente la asignación de dirección IP a través de un servidor DHCP. Si por el contrario se elige asignación estática entonces se deben colocar manualmente los siguientes parámetros.
  - IP address.
  - Subset Mask (Mascara de Subred[35]).
  - Default Router: Es la dirección del enrutador por el cual debe salir el usuario hacia otra red.
  - DNS primario (Servidor de Nombres).
  - DNS Secundario (Opcional).

[35] Mecanismo para dividir una red en varias subredes para darle características de privacidad y administración a la red total.

- El Dominio o Dirección IP del *Servidor SIP.*
- El Dominio o Dirección IP del *Outbound Proxy* [36]si es necesario.
- El *SIP User ID*. Es el identificador de Usuario. Este es el nombre que se registra en la base de usuarios del servidor SIP. Para poder iniciar una sesión debe existir ese nombre ya registrado en la base de datos.
- *El Authenticate ID.* Este nombre puede ser el mismo *Sip User ID.*
- *El Authentícate Password.* Es el password que también esta en la base de datos del servidor Sip. Para poder iniciar una sesión esta contraseña debe coincidir con la de la base de datos.
- *Name.* Este es el nombre a mostrar a los demás usuarios cuando tienen una llamada entrante del usuario.

Otras opciones avanzadas de configuración consisten en la elección de los codecs de audio y video según la disposición de ancho de banda de la red donde se encuentra conectado el usuario, si se habilita el registro automático al servidor SIP, si se reinicia el equipo al no poderse registrar, los puertos UDP (SIP:5060 default, RTP:8000 default), si se habilita el uso de puertos aleatorios, si se suprime el silencio, si existe un servidor STUN[37] cuando se encuentra en un escenario que cuenta con NAT[38]/Firewall, y otras opciones que dependen de la funcionalidad del equipo que se disponga.

Para este trabajo de investigación se configuraron y se usaron 2 marcas de ATA's: Cisco ATA186 y GrandStream Handy Tone-286. Por la funcionalidad, fácil manejo, buen desempeño y bajo costo se decidió trabajar con los segundos. En la figura 25 se adjunta una tabla con los comandos que se pueden ejecutar en el ATA con el teléfono análogo marcando cada uno de estos.

[36] Servidor proxy de respaldo utilizado para manejar el tráfico saliente.
[37] Cruce Simple de Paquetes UDP a través de un NAT.
[38] Traductor de Direcciones de Red de Trabajo.

Figura 24. Menú de configuración del ata 286

Menu	Voice Prompt	User's Options
Main Menu	"Enter a Main Option"	Enter '*' to menu_01 Enter 00-06, 99 menu option
01	"DHCP Mode", "Static IP Mode"	Enter '9' to toggle the selection
02	"IP Address " + IP address	It will prompt you with the current IP address. Enter 12 digit new IP address if in Static IP Mode
03	"Subnet " + IP address	Same as menu 02
04	"Gateway " + IP address	Same as menu 02
05	"DNS Server " + IP address	Same as menu 02
06	"TFTP Server " + IP address	Same as menu 02
47	"Direct IP Calling"	When entered, you will prompt a dialtone, then enter 12 digit IP address This menu can be also entered by pressing the button again
86	"Voice Messages Pending" "No Voice Messages"	Enter 9 to dial pre-configured phone number to retrieve VM
99	"RESET"	Enter '9' to confirm the RESET Enter MAC address to restore factory default setting
	"Invalid Entry"	Automatically return to Main Menu

Fuente: HandyTone User Manual [en línea]. Chicago : Grandstream Networks inc, 2002. [Citado 11 de feb, 2004]. Disponible por internet : http://www.grandstream.com/user_manuals/HandyTone.

5. 11. 2 Teléfonos software. Estas son aplicaciones de software diseñadas para la telefonía digital con los protocolos de VoIP. En el Internet existe gran variedad de estos y se pueden bajar gratuitamente e instalar en el PC. Esta opción es muy útil y mucho más económica que las otras. Es ideal para personas que permanecen la mayor cantidad del tiempo frente a un computador ya que con solo configurarlo una vez solo se necesita que la persona encienda su equipo o ejecute la aplicación y este intentara iniciar la sesión en el servidor SIP. Si el software está bien configurado entonces el programa no tendrá ningún inconveniente en registrarse y estar disponible para todos los usuarios.

Hay de todas las gamas en el Internet. Después de probar con varias aplicaciones se escogió una en especial que además de ser gratuita, es bastante configurable para los distintos escenarios que se puedan presentar, entrega reportes de diagnostico, tiene la posibilidad de varias líneas de voz y otras funciones que lo hacen bastante útil. La aplicación se llama *X-Lite* y se puede bajar de la dirección de Internet *www.xten.com*. Esta aplicación cuenta con un menú de configuración bastante amplio que permite ingresar todos los campos mencionados en los ATA`s y muchos otros relativos a opciones de usuario, reportes, diagnósticos, codecs, tiene la posibilidad de configurar 10 dominios para 10 proveedores de servicios de VoIP, libreta de teléfonos, etc. Los SoftPhones que fueron probados en este trabajo de investigación se señalan a continuación.

- LipZ (Linux).
- Kphone (Linux).
- SJPhone (Windows).
- X-Lite (Windows).

Para cualquiera de estas aplicaciones se debe contar con unos audífonos y un micrófono para poder escuchar y enviar audio en cada sesión.

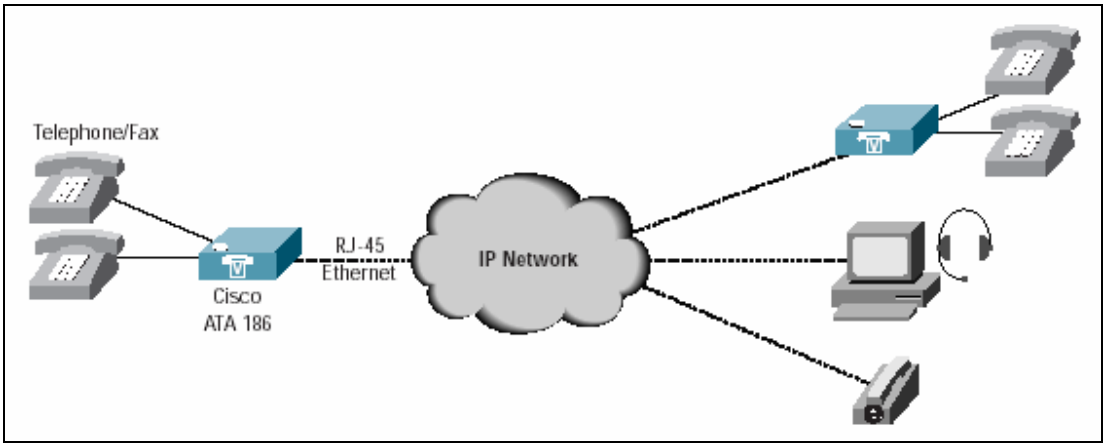
5. 11. 3 Teléfonos hardware. Esta es la opción más eficiente y más robusta de las tres, pero así mismo es la más costosa por la tecnología con que cuenta y a demás que no son equipos muy comerciales en nuestro país lo cual hace su precio aun más elevado. Estos equipos cuentan con una pantalla de cristal líquido en la que se puede visualizar varia información tanto del usuario que llama como del que recibe la llamada; cronómetros de llamadas, registro de llamadas, libreta de teléfonos, y varias opciones que los hacen

supremamente funcionales. Los principales distribuidores de estos equipos a nivel mundial son

- Cisco Systems.
- DIGiCOM
- Siemens.
- Prosip.
- GrandStream.
- Snom.

En este trabajo de investigación no se trabajó con ninguno de estos equipos ya que no se disponía de ninguno de los recursos económicos para adquirirlos ya que su costo supera los 200 dólares. Además se pretende que para los usuarios y clientes de este tipo de servicios puede ser mucho más llamativa económicamente cualquiera de las dos opciones anteriores mientras que se les garantice un buen desempeño.

Figura 25. Esquema general de ínterconectividad

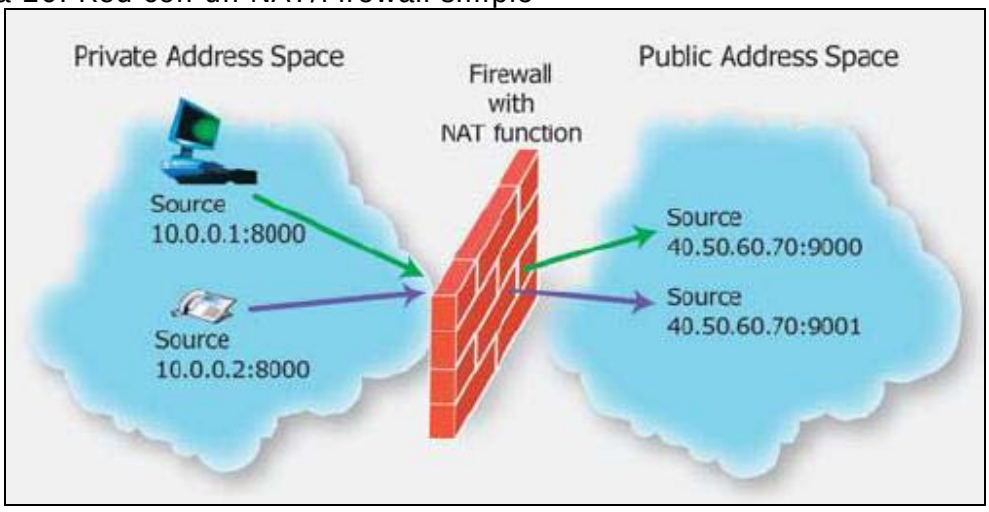


Fuente: Cisco ATA 186 [en línea]. Stanford : Cisco Systems, 2003. [Citado 11 de feb, 2004]. Disponible por internet : www.cisco.com/warp/public/cc/pd/as/180/ 186.

5. 12 ESCENARIOS Y SOLUCIONES PARA APLICACIONES SIP QUE CORREN DENTRO DE UN NAT/FIREWALL.

5. 12. 1 Introducción. En el momento de enviar paquetes a través de un NAT/Firewall es necesario prestar mucha atención a cada una de las variables implicadas en el proceso. Es particularmente engorroso en el caso de comunicaciones multimedia e interactivas manejadas por el protocolo SIP. Se han propuesto unas cuantas soluciones para lograr este cometido como son utilizar los protocolos STUN (Simple Traversal of UDP Trought NAT), TURN (Traversal Using Relay NAT) y MIDCOM, además de otros opciones como el uso de algoritmos SIP, extensiones SDP para NAT´s, extensiones SIP para NAT´s, túneles, etc. Este problema es complicado ya que se presentan una gran variedad de escenarios que serán descritos a continuación.

Figura 26. Red con un NAT/Firewall simple



Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

5. 12. 2 Clases de NAT's.

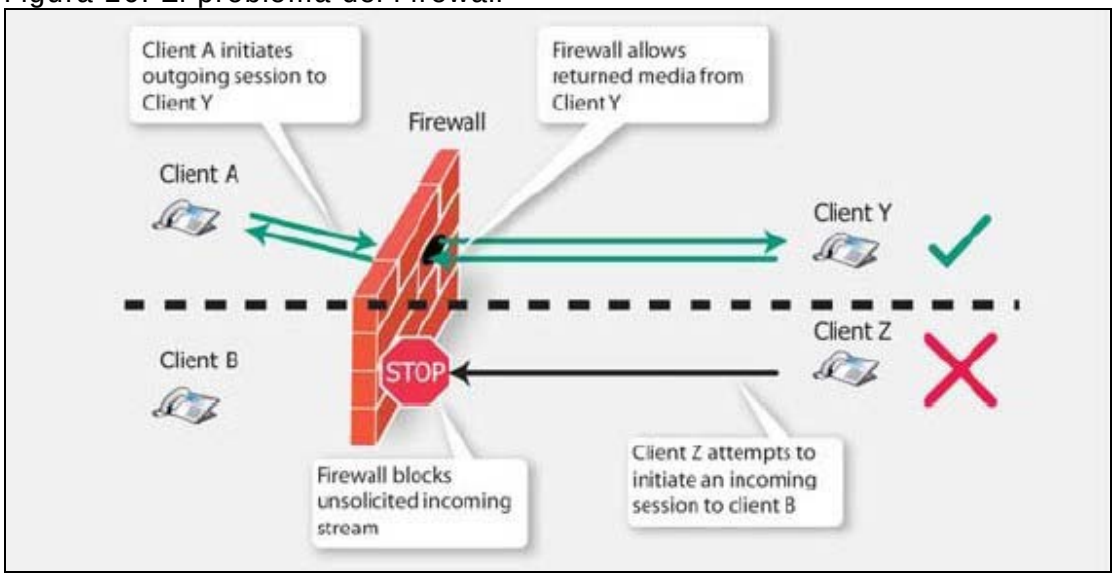
- **Full-cone NAT**. Un Puerto es asignado cuando un dispositivo (PC SoftPhone, ATA, SIP HardPhone) detrás del NAT (Red Privada) envía un paquete por primera vez hacia el espacio público. El NAT de aquí en adelante permite solo el paso por ese puerto para peticiones que tengan como destino el dispositivo para quien fue creado este puerto. Para este caso el NAT no examina cual es el origen de los paquetes entrantes.

- **Restricted-cone NAT**. Un Puerto es asignado cuando un dispositivo (PC SoftPhone, ATA, SIP HardPhone) detrás del NAT (Red Privada) envía un paquete de invitación por primera vez hacia otra red en el espacio público. El NAT de aquí en adelante permite solo el paso por ese puerto para paquetes que tengan como destino el dispositivo para quien fue creado este puerto. Para este caso el NAT examina si el origen de los paquetes pertenece a la red que recibió el paquete de invitación. De no ser así no permite su paso.

- **Port restricted-cone NAT**. Un Puerto es asignado cuando un dispositivo (PC SoftPhone, ATA, SIP HardPhone) detrás del NAT (Red Privada) envía un paquete de invitación por primera vez a un dispositivo (usuario) en otra red en el espacio público. El NAT de aquí en adelante permite solo el paso por ese puerto para paquetes que tengan como destino el dispositivo para quien fue creado este puerto. Para este caso el NAT examina si el origen de los paquetes recibió el paquete de invitación, es decir, solo los usuarios de esa red que hayan recibido la invitación pueden pasar sus paquetes hacia su destino a través del NAT. En caso de ser Multicast, varios dispositivos lo podrán hacer. De no ser así no permite su paso.

- **Symmetric NAT**. Un Puerto es asignado cada vez que un dispositivo (PC SoftPhone, ATA, SIP HardPhone) detrás del NAT (Red Privada) envíe un paquete de invitación a un nuevo dispositivo (usuario) en otra red. El NAT de aquí en adelante permite solo el paso por ese puerto para paquetes que tengan como destino el dispositivo para quien fue creado este puerto. Para este caso el NAT examina si el origen de los paquetes recibió el paquete de invitación, es decir, solo los usuarios de esa red que hayan recibido la invitación pueden pasar sus paquetes hacia su destino a través del NAT. En caso de ser Multicast, varios dispositivos lo podrán hacer. De no ser así no permite su paso. Lo que hace difícil el cruce del NAT cuando es simétrico es la regla de creación de puertos, puesto que a diferencia de las otras clases de NAT's, un nuevo puerto será creado cada vez que un dispositivo detrás del NAT envié un paquete de invitación.

Figura 26. El problema del Firewall



Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

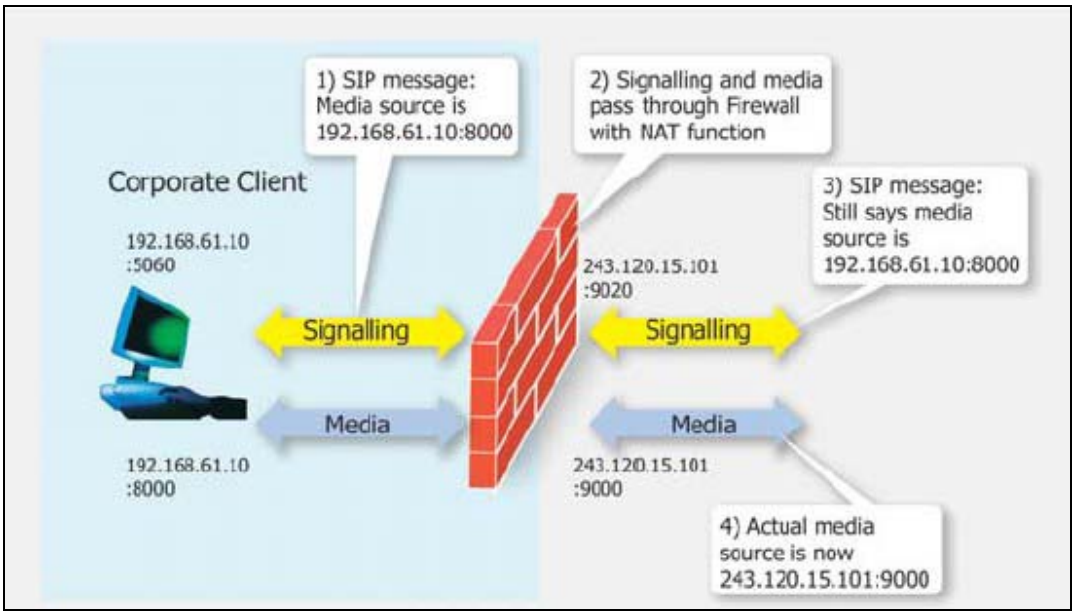
5. 12. 3 Qué problema introduce en el señalamiento SIP y flujo de multimedia la existencia de un Firewall?. El rol de un Firewall como sistema de seguridad es proteger la red de ser accedida por fuentes no autorizadas. Este realiza el bloqueo de tráfico basado en 3 parámetros: La fuente, el destino y el tipo de tráfico. Además los Firewalls también toman decisiones basados en la dirección de flujo de tráfico. Típicamente el tráfico entrante de fuentes no confiables de la red pública es solamente permitido si una sesión es iniciada por un dispositivo dentro de la red privada confiable.

La comunicación basada en el protocolo SIP, al igual que la mayoría de las comunicaciones, están basadas en llamadas entrantes no solicitadas por un rango de fuentes no necesariamente confiables. Es por esto que las políticas del Firewall son un problema para el funcionamiento del los servicios de VoIP, y a su vez, el solucionar este problema abriendo puertos para el tráfico entrante introduce problemas de seguridad para la red.

5. 12. 4 Qué problemas introduce en el señalamiento SIP y flujo de multimedia la existencia de un NAT?. Básicamente son dos problemas.

- Tráfico de Salida: Cuando el usuario envía un mensaje SIP hacia el exterior del NAT el mensaje contiene como dirección fuente la dirección IP privada de este, así que nunca va recibir ninguna respuesta puesto que esta no se puede enrutar.
- Tráfico de Entrada: Las relaciones que hace el NAT entre las direcciones y puertos públicos y las direcciones y puertos privados solo ocurre cuando el usuario al interior de la red envía un pedido, así que mientras el usuario dentro de los límites del NAT no envíe una petición este es invisible desde la red pública

Figura 27. Problemas de señalamiento SIP debido a un NAT.



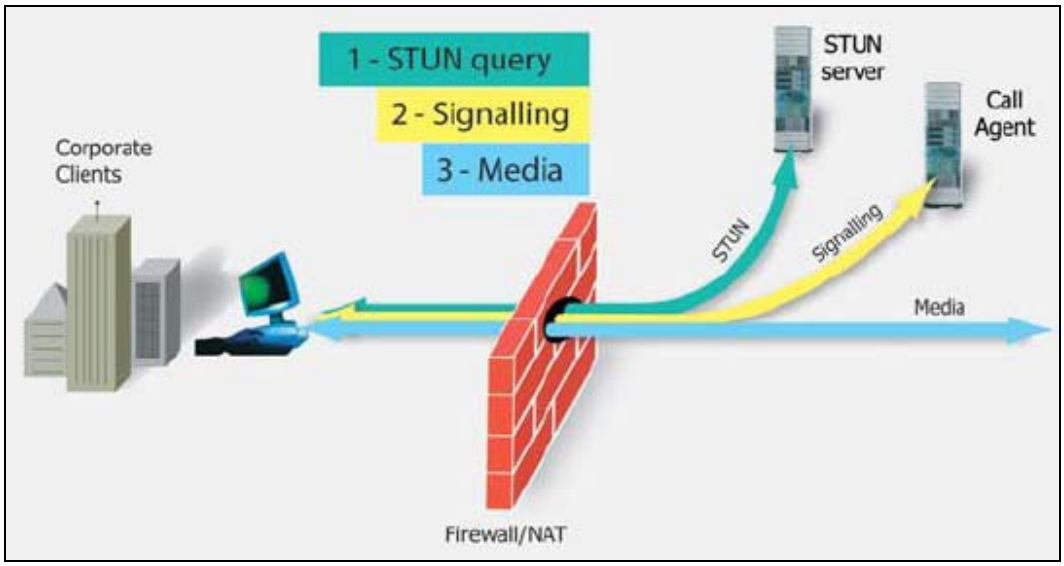
Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

5. 12. 5 Soluciones al problema introducido por un NAT/Firewall.

- **Solución UPnP**. El objetivo predominante de esta tecnología son los usuarios residenciales y de oficina. Esta tecnología le permite a clientes que se encuentran dentro del límite de un NAT/FW configurar componentes de red para que descubran su dirección y puerto IP en el lado público de la red para poder hacer una correcta señalización y establecer la sesión con los parámetros reales (Públicos). Esto es posible si se cuenta con componentes (Incluidos Nat y firewalls) equipados con el software UPnP.

- **Solución STUN (Simple Traversal of UDP Through Nat)**. El protocolo STUN le permite al cliente descubrir si está detrás de un NAT y si lo está, de que tipo es. El protocolo STUN le permite al cliente conocer su dirección pública en el Internet estando detrás de un NAT (exceptuando el tipo de NAT simétrico). Cuando el cliente se inicializa, lo primero que hace es utilizar su compatibilidad con el protocolo STUN para determinar en que tipo de NAT se encuentra. Este chequeo sólo se realiza en la inicialización del equipo. Una vez que el tipo de NAT ha sido descubierto, la operación de ahí en adelante depende exclusivamente del resultado que descubrió. Si el usuario descubrió que no se encuentra detrás de un NAT, ningún procesamiento adicional es requerido.

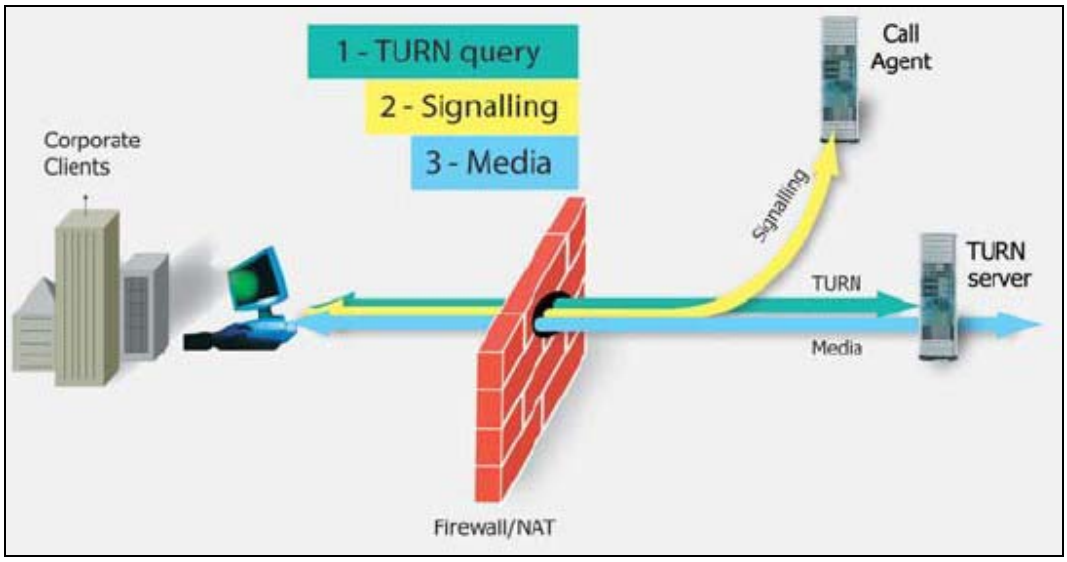
Figura 28. Solución STUN



Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

- **Solución TURN (Traversal Using Relay NATs)**. Esta es una solución propuesta para el problema de los NAT simétricos. El TURN se ubica en un servidor de Media insertado en la ruta del tráfico de media. Este se puede ubicar en el cliente DMZ o en el proveedor de servicios de red. Los clientes SIP envían un paquete exploratorio al servidor TURN en el cual estén habilitados y este les responde con la Dirección Publica y el puerto usado por el NAT en esa sesión. Esta información es usada para el establecimiento de la llamada y del flujo de media subsiguiente. La ventaja de este sistema es que no hay cambio en la dirección destino usada por el NAT para el establecimiento de la llamada y para el flujo de media. Por esta razón, el NAT simétrico puede ser usado.

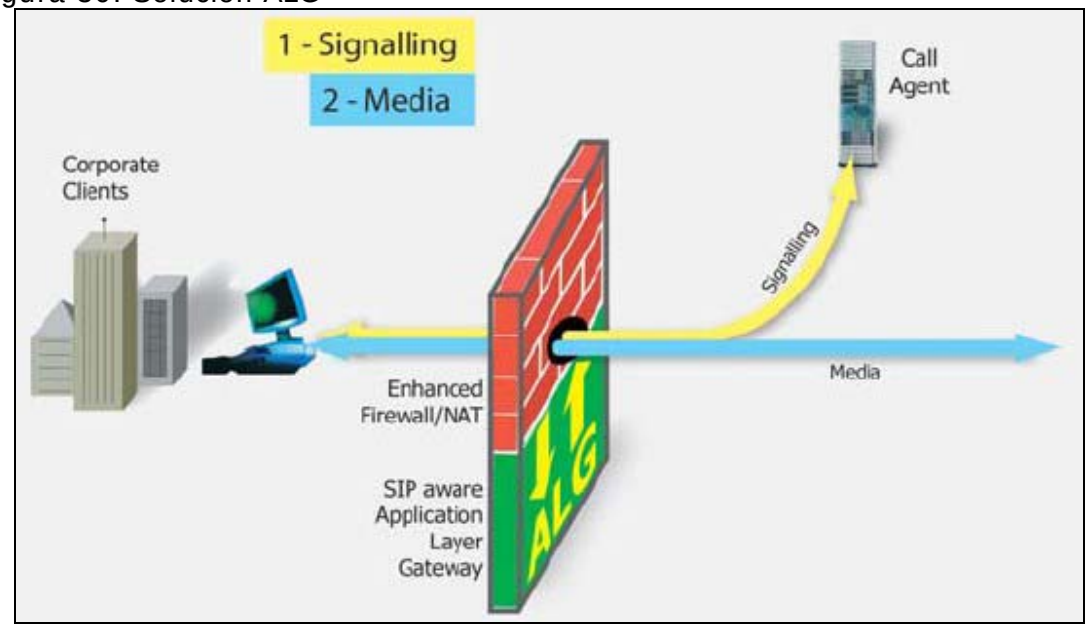
Figura 29. Solución TURN



Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

- **Solución ALG (Application Layer Gateway)**. Con esta solución, la empresa actualiza su Firewall o compra uno nuevo que le permita correr un software integrado llamado SIP ALG. Con esta actualización, el NAT/Firewall examina cada pedido SIP y modifica los campos de Contacto, Via y SDP con el fin de que la Dirección IP fuente corresponda al a Dirección IP publica y el puerto usado por el NAT para el manejo de las diferentes etapas de una sesión SIP. Esta opción no se recomienda si los mensajes SIP van encriptados, a menos que el NAT/Firewall actúe como SIP proxy. Además, la empresa disemina servidores proxy a través de toda su red. El NAT es configurado con un mapeo estático para cada uno de estos servidores internos al enlazarlos con la red pública. El esquema general se muestra en la figura 30.

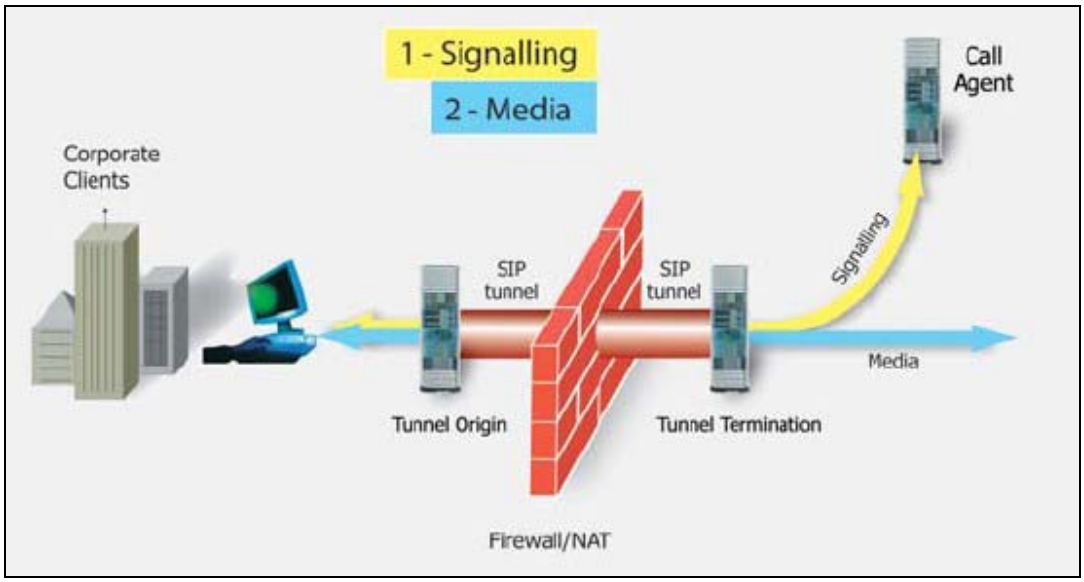
Figura 30. Solución ALG



Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

- **Técnicas de Túneles**. Este método propone cruzar el NAT/Firewall mediante la creación de un túnel para el traspaso de la señalización y el trafico de media a través de las instalaciones NAT/Firewall existente hacia un servidor en el espacio de direcciones público. Este método requiere un nuevo servidor dentro de la red privada y otro en el espacio publico. Estos dispositivos crean un túnel entre ellos para el paso de la señalización y el tráfico de media. El servidor externo modifica la señalización para reflejar la dirección IP pública y los puertos usados por el NAT. Esto permite al servicio de VoIP tanto las llamadas salientes como las entrantes. De cualquier forma, esta propuesta crea un hueco en la seguridad que puede significar ataques por parte de las fuentes en el espacio público. Además, el método provoca un retraso en el flujo de media lo cual puede disminuir la calidad del servicio.

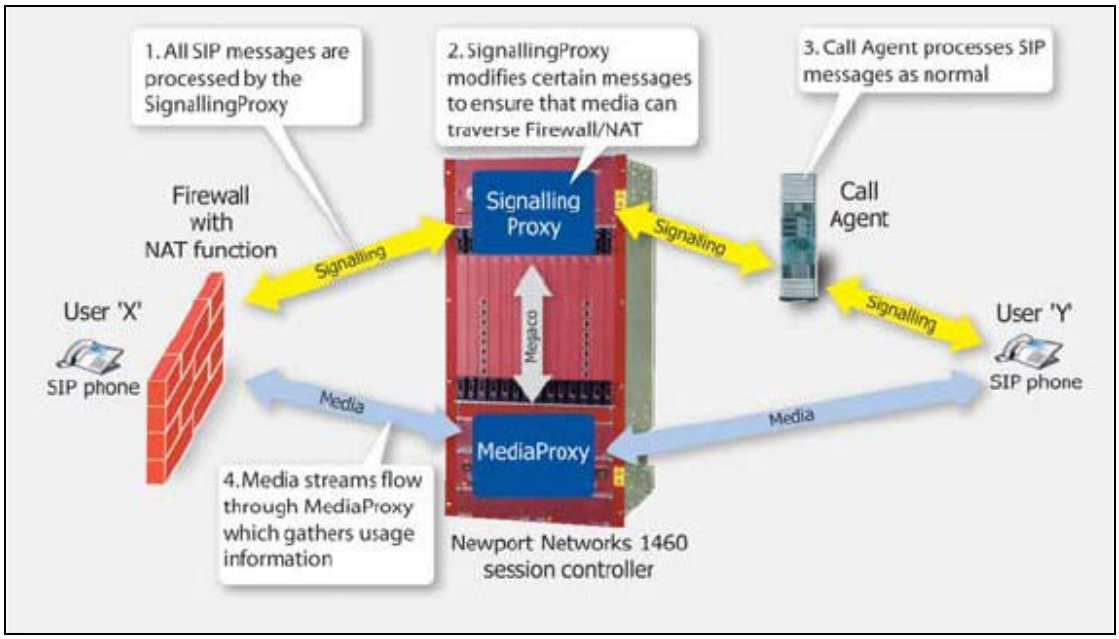
Figura 31. Técnica de túnel.



Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

- **Solución B2BUAWM (Back to Back User Agent With Media)**. Este elemento tramita todo el tráfico de multimedia y mensajes SIP adentro y hacia afuera la red. Como resultado de esto, el administrador del Firewall puede configurarlo para que permita todo el tráfico de entrada y salida asignado a este elemento. Similarmente, si un NAT es usado, se realiza un mapeo estático relacionando una dirección pública a la privada en la que se encuentra este elemento, o también, se le asignará a este un rango de puertos de la dirección IP pública. Esta solución puede ser usada al límite de la red privada o se puede implementar como un servidor en el espacio publico para satisfacer a muchos espacios limitados por diferentes NAT; de esta manera podemos llamarlo B2BUAWM interno o externo. En la figura 33 se muestra un diagrama general y de funcionamiento de ésta solución.

Figura 32. Solución B2BUAWM.



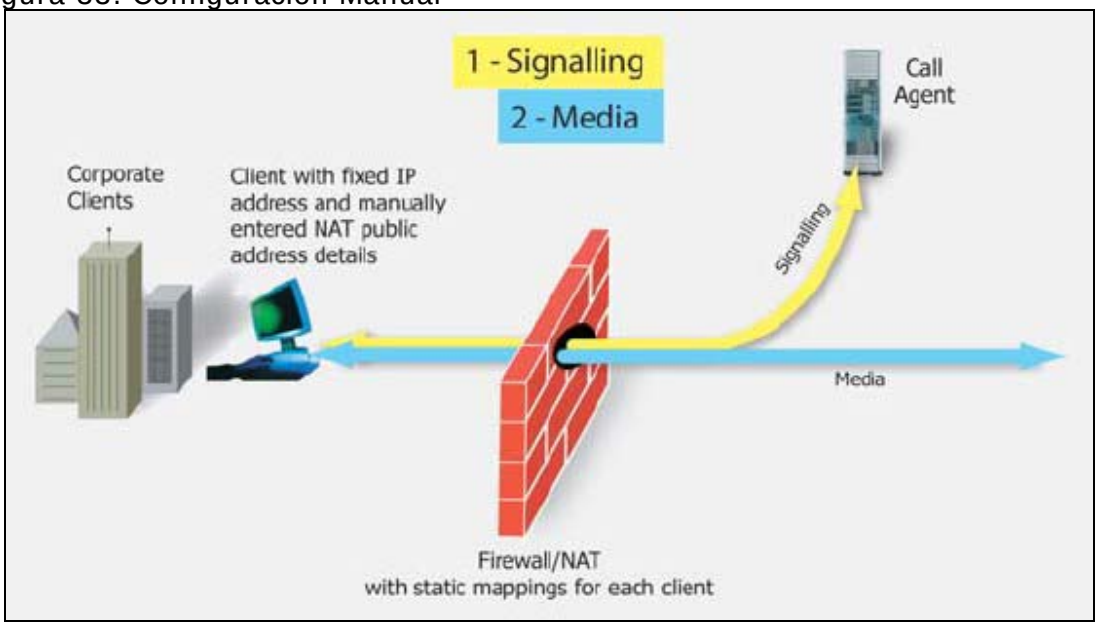
Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

- **Prerrequisitos para el señalamiento:**
  - Esta solución recae en el principio que en cuanto a las comunicaciones dentro de la red empresarial son permitidas las conexiones hacia afuera y sus correspondientes respuestas. Esto le permite a los usuarios dentro de la red empresarial mantener una conexión con el servidor de señalamiento mediante un mecanismo de *keep-alive.*
  - Todos los mensajes de señalamiento deben viajar a través del proxy de señalamiento. El servidor proxy de señalamiento SIP en el cual los usuarios están registrados debe ser aquel por el cual pasé todo el tráfico de las llamadas entrantes y salientes.
  - El servidor proxy de señalamiento SIP debe estar a un salto de distancia de los usuarios.
  - El puerto de destino de los pedidos en el servidor de señalamiento Proxy debe ser el mismo de la fuente que envía la respuesta.

- **Prerrequisitos para el envío de información multimedia:**
  - Cualquier información multimedia que atraviese el NAT desde el lado privado de la red debe pasar a través del servidor proxy RTP.
  - Las direcciones y los puertos en el servidor proxy RTP pueden ser asignados durante la negociación de conexión o antes de ella.
  - El servidor proxy RTP debe saber dónde enviar la información multimedia que recibe. Por ejemplo, si está actuando como puente entre dos clientes privados que se encuentran en distinta red privada, el servidor debe saber la dirección y el puerto públicos de los usuarios antes de recibir cualquier información multimedia.
  - Los puertos de envío y recepción de multimedia en los usuarios deben estar configurados de la misma forma que los servidores proxy RTP.

- **Configuración Manual**. En este método, el cliente es manualmente configurado con detalles de la dirección IP pública y puertos que el NAT utilizara para la señalización y trafico de media. El NAT además es manualmente configurado con un mapeo estático para cada cliente. Este método requiere que el cliente deba tener una dirección IP fija y puertos fijos para la señalización y el tráfico de media SIP.

Figura 33. Configuración Manual



Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

Muchos NAT´s residenciales permiten configurarse con un host DMZ. Este servicio recibe todos los paquetes que no están asociados con una conexión de salida ya establecida anteriormente. El NAT también le permite al usuario saber la dirección IP que le fue asignada por su proveedor de

Internet. El procedimiento para la configuración es simple. Primero, se determina la dirección IP asignada al usuario por su proveedor de Internet (Dirección Pública); esto se logra mirando la configuración del NAT. Segundo, se determina la dirección IP que le fue asignada al teléfono SIP (Dirección del Teléfono). Luego se configura el host DMZ para que envíe al teléfono SIP todos los paquetes de tráfico entrante no asociados a una conexión previamente realizada. Por último, se configura el teléfono SIP para que utilice la dirección pública para todos los mensajes SIP y SDP.

5. 12. 6 Escenarios y soluciones posibles de implementar. A continuación se presentan los escenarios que se pueden presentar por la combinación de tipos de redes, tipos de NTA/Firewall, tipos de clientes y políticas de seguridad. Para cada uno de estos se presentan algunas soluciones de las explicadas anteriormente. La idea es permitir el establecimiento de sesiones a través del protocolo SIP sin importar las características que presenten los diferentes escenarios.

- **Escenario I. Red residencial con un NAT simple.** En este escenario, un usuario tiene una conexión de banda ancha a Internet utilizando cable modem o xDSL. El usuario además ha adquirido un enrutador para que varios de los computadores que se encuentran dentro de su red residencial tengan acceso al servicio de Internet y queden protegidos. Estos dispositivos comúnmente fabricados por empresas como NetGear, 3Com, Lynksys, 2Wire y Netopia, poseen en su estructura un NAT, un Firewall simple, un servidor y clientes DHCP, y tienen incorporado un switch ethernet de algún tipo. El Firewall generalmente permite todo el tráfico de salida, pero deshabilita el tráfico de entrada a menos que se haya configurado un puerto específico o un host DMZ. El tratamiento NAT de los paquetes UDP en estos dispositivos varía dependiendo del mismo. Los tipos

más comunes de NAT´s que poseen estos dispositivos son *Full Cone NAT* y *Restrincted Cone NAT*. El usuario desea conectarse a un servicio de un proveedor como net2phone o deltathree. La conexión entre los usuarios y el proveedor es a través de cable modem o xDSL, sobre la red de Internet. El usuario puede tener varios computadores personales en su hogar accesando al servicio, pero a su vez no estar relacionados en ninguna forma. Este escenario también incluye el caso donde se tengan teléfonos SIP de hardware.

Soluciones posibles.

- **Configuración manual.**
- **Clientes que soporten el protocolo STUN.** La segunda solución para este escenario es adquirir un teléfono SIP que soporte el protocolo STUN, y opcionalmente, extensiones SDP para NAT, extensiones SDP para multimedia orientada a conexión y extensiones SIP para NAT.

- **Escenario II. Empresas no corporativas.** Una empresa no corporativa consiste en usuarios que desean acceder a un servicio de telefonía por Internet que ofrece un proveedor externo. Sin embargo, las empresas utilizan un NAT/Firewall. La empresa no ha montado en su infraestructura un sistema de VoIP, no ha añadido ninguna infraestructura y no ha cambiado su configuración para soportar el protocolo SIP ni le interesa hacerlo. Este caso en gran parte se parece al escenario residencial y casi todas sus soluciones pueden ser usadas en este, con unas leves diferencias.

Primero, la solución de configuración de la red no está disponible ya que la empresa no les permite a sus empleados tener ningún control

administrativo sobre el NAT. Segundo, el NAT empresarial comúnmente posee una funcionalidad de Firewall, lo cual lo hace altamente restrictivo; inclusive, administrativamente se pudo haber bloqueado todo el tráfico UDP de entrada y salida. En este caso, la única solución es utilizar túneles encriptados o redes privadas virtuales (VPN). Sin embargo, lo anterior puede representar e introducir debilidades en el sistema de seguridad lo cual iría en contra de la política que la incorporación de un NAT/Firewall propende. Si el NAT/Firewall empresarial permite todo el tráfico UDP y TCP de salida, entonces todas las soluciones para el escenario residencial pueden ser utilizadas y funcionarán correctamente.

- **Escenario III. Empresas corporativas.** En este escenario, existe una empresa que desea desarrollar e implementar servicios de telefonía utilizando el protocolo SIP. En este caso no se cuenta con ningún proveedor público, lo cual hace que la empresa tome absoluto control sobre el servicio. Dada esta circunstancia, los administradores del Firewall empresarial poseen la habilidad de manipular su configuración si es necesario, o añadir y desarrollar elementos adicionales a su red interna.

Soluciones posibles.

- **SIP ALG**. El proceso de registro se hace enteramente dentro de la red empresarial privada. Los clientes SIP dentro de la red pueden comunicarse unos con otros directamente. Los clientes SIP que deseen comunicarse con el mundo exterior, pueden hacerlo a través del servidor SIP Proxy de la empresa. Cuando se inicializa una sesión desde fuera de la red empresarial, el NAT/Firewall re-escribe porciones del mensaje SIP de invitación para que en él aparezca la dirección IP pública. El NAT/Firewall también asigna un par de puertos públicos para las transacciones RTP y RTCP, mapeándolos con las direcciones y puertos

privados, permitiendo la entrada de todo el tráfico que llega a estos puertos desde el Internet. Como ejemplo se muestra siguiente mensaje invitación en su forma original (Figura 34) y en su forma re-escrita (Figura 35).

Figura 34. Forma original del mensaje de invitación (ALG)

```
INVITE sip:user@domain SIP/2.0
From: sip:user@work.com;tag=88asd
To: sip:user@domain
Call-ID: 98asd6asd60099
CSeq: 987769 INVITE
Via: SIP/2.0/UDP 10.1.1.5
Via: SIP/2.0/UDP proxy1.work.com;maddr=10.1.1.1
Record-Route: proxy1.work.com
Contact: sip:10.1.1.5:5060
Content-Type: application/sdp
o=aa 2890844526 2890842807 IN IP4 10.1.1.5
c=IN IP4 10.1.1.5
m=audio 17832 RTP/AVP 0
```

Fuente: NAT and Firewall Scenarios and Solutions for SIP [en línea]. East Hanover : IETF, 2002. [Citado 5 de abr, 2004]. Disponible por internet : http://www.ietf.org/internet-drafts/draft-ietf-sipping-nat-scenarios-00.txt.

Figura 35. Forma re-escrita del mensaje de invitación (ALG)

```
INVITE sip:user@domain SIP/2.0
  From: sip:user@work.com;tag=88asd
  To: sip:user@domain
  Call-ID: 98asd6asd60099
  CSeq: 987769 INVITE
  Via: SIP/2.0/UDP 10.1.1.5
  Via: SIP/2.0/UDP proxy1.work.com;maddr=1.2.3.4:5060
  Record-Route: proxy1.work.com
  Contact: sip:1.2.3.6:7843
  Content-Type: application/sdp
  o=aa 2890844526 2890842807 IN IP4 10.1.1.5
  c=IN IP4 1.2.3.4
  m=audio 5678 RTP/AVP 0
```

Fuente: NAT and Firewall Scenarios and Solutions for SIP [en línea]. East Hanover : IETF, 2002. [Citado 5 de abr, 2004]. Disponible por internet : http://www.ietf.org/internet-drafts/draft-ietf-sipping-nat-scenarios-00.txt.

De la misma forma cuando se recibe una invitación a sesión, el NAT/Firewall re-escribe el mensaje de respuesta en la parte de descripción de sesión, por ende, el NAT/Firewall debe estar preparado para re-escribir una oferta en un mensaje 200 OK y una respuesta en un mensaje ACK.

- **B2BUAWM interno.** En esta solución, la empresa no tiene la necesidad de cambiar su NAT/Firewall para que soporte ALG SIP. En cambio, se añade un elemento adicional dentro de la red empresarial, el cual es llamado comúnmente B2BUAWM (Back to Back User Agent With Media).

- **Escenario IV. Servicios de Outsourcing.** En este escenario, conocido también como CENTREX, la compañía desea implementar el sistema de telefonía por Internet, pero lo subcontrata con un proveedor de servicios de VoIP.

  - **SIP ALG.** En esta solución, la empresa actualiza su NAT/Firewall para que soporte del método SIP ALG. A diferencia de las empresas corporativas, no hay necesidad de diseminar servidores proxy ni otros elementos dentro de la red. Los clientes de la empresa se registran directamente con los servidores proxy que posee la compañía de Outsorcing. Esto significa que el SIP ALG necesita re-escribir los mensajes de registro además de los mensajes de invitación, 200 OK y ACK. En contraste con el caso corporativo los mensajes de registro si traspasan el NAT/Firewall. El diagrama general este caso está expuesto la figura 30.

- **B2BUAWM externo.** En esta solución, el proveedor del servicio utiliza un agente B2BUAWM en vez de un SIP Proxy. Esto puede verse como una integración de un servidor Proxy y un servidor TURN como una aplicación para una solución específica. Con esta solución, la empresa no tiene la necesidad de integrar un SIP ALG en su red.

6. METODOLOGÍA

6. 1 DOCUMENTACIÓN Y ADQUISICIÓN DE INFORMACIÓN.

Se estudiaron las teorías de establecimiento de sesiones, escenarios de uso, antecedentes y debilidades referentes al Protocolo de Inicialización de Sesión (SIP) mediante documentos técnicos como el RFC 3261, en el cual se expone de manera extensa las bases y documentos didácticos desarrollados para dar una visión clara sobre este.

Se estudiaron los documentos técnicos referentes a los protocolos que complementan al SIP para lograr el desarrollo del objetivo propuesto. Estos documentos fueron: RFC 2327 (SDP), RFC 1889 (RTP) y RFC 3605 (RTCP).

Se revisó la documentación referente al servidor HTTP APACHE para lograr configurar el servicio web que complementa el sistema que se configuró.

Se estudió el funcionamiento del entorno de bases de datos MySQL[39] y el juego de instrucciones SQL para lograr la configuración del servicio de ubicación del servidor SIP.

[39] Gestor gratuito de Bases de datos de buena capacidad de almacenamiento de información y manejo de comandos de consulta SQL.

Utilizando herramientas de Internet como los buscadores Google™ y MSN™ se logró encontrar un enrutador de paquetes SIP gratuito el cual posee la flexibilidad necesaria para los intereses de este proyecto; este software se llama SIP Express Router (SER).

Gracias a la documentación relacionada con el SER se obtuvo la información necesaria para lograr tener los conocimientos que luego permitieron la configuración del servicio.

Se acudió a la documentación relacionada con el pre-procesador de hipertexto PHP con el objeto de obtener información para programar la interfase web del servidor SIP con todas las políticas mínimas de seguridad para garantizar al usuario un manejo seguro de su información.

Se estudiaron las posibilidades en cuanto a recursos de ínterconectividad para luego escoger las soluciones que mejor se adaptaran al sistema y a la economía del proyecto.

6. 2 CONFIGURACIÓN, DESARROLLO COMPLEMENTARIO E IMPLEMENTACIÓN DEL SERVIDOR SIP

Se configuró el software SER en un PC de la Universidad Autónoma de Occidente.

Se configuró el servidor MySQL y el pre-procesador de hypertexto PHP para funcionar en conjunto con es SIP Express Router (SER).

Se desarrolló la interfase web utilizando HTML, PHP, compatibilidad PHP con bases de datos de MySQL y elementos Flash.

6. 3 DESARROLLO DE PRUEBAS

Primero que todo, se realizaron pruebas de funcionamiento del sistema dentro de la red de área local de la Universidad Autónoma de Occidente para hacer un diagnóstico del funcionamiento del servidor SIP. Durante este periodo se dio un proceso de depuración de todos los elementos del sistema.

Finalmente se adquirió un nombre de dominio, una dirección IP fija y una conexión de banda ancha por fuera de la Universidad Autónoma de Occidente y se probó satisfactoriamente el sistema entre usuarios de ADSL[40] y Cable MODEM en Cali, Bogotá y Medellín.

[40] Línea de suscripción digital asimétrica.

7. RESULTADOS

A continuación se mostrara el desarrollo paso por paso para lograr la implementación del servidor SIP con sus respectivos complementos que lo hacen como resultado supremamente funcional.

7. 1 SER (SIP EXPRESS ROUTER)

7. 1. 1 Descripción. El SER es un servidor de capacidad industrial de VoIP basado en el Protocolo de Inicialización de Sesión (SIP). Está diseñado para expandir infraestructuras de telefonía IP a larga escala. Este servidor lleva un registro de los usuarios, inicializa sesiones de VoIP, permite mensajería instantánea y crea un espacio para el desarrollo de nuevas aplicaciones en el campo. Su interoperabilidad ya probada garantiza una integración sin igual con componentes de cualquier fabricante, descentralizando las comunicaciones. El SER ha sido parte de varias pruebas de interoperabilidad con gran éxito, en las cuales se ha trabajado con productos de los mejores fabricantes de dispositivos SIP. Este servidor permite una conexión flexible con nuevas aplicaciones. Terceras personas pueden fácilmente enlazar sus plug-ins [41]con el código del servidor y proveer a través de él servicios avanzados y específicos. Por ejemplo, con una CPU dual de $3000 USD, el SER es capaz de proveer servicios de telefonía IP en un área tan grande como Cali en las horas pico de utilización del servicio telefónico. Inclusive, instalado en un computador de mano IPAQ PDA, el servidor puede procesar hasta 150 llamadas por segundo.

[41] Módulo opcional que puede ser agregado a una aplicación para realizar una acción específica.

El servidor SER es extremadamente configurable, lo cual permite la creación de muchas políticas de enrutamiento y admisión, además permite configurar servicios novedosos y específicos. Su configurabilidad le permite interpretar varios roles, tales como barreras de seguridad de una red, servidor de aplicaciones o como un enlace y guardia de una red pública telefónica conmutada (PSTN).

Basado en los últimos estándares, el SIP Express Router incluye soporte para un servidor de registro, proxy y servidor de re-dirección. También puede actuar como un servidor de aplicación con soporte para CPL, mensajería instantánea y residencial (IM&P) incluyendo una puerta de enlace 2G/SMS, lenguaje de control de políticas de llamada, traductor de números de llamada, planes privados de llamada y servicios de autorización y autentificación (AAA). SER corre bajo diversas plataformas como Sun/Solaris, PC/Linux, IPAQ/Linux y soporta tanto la versión IPv4 como la IPv6.

7. 1. 2 Escenarios de uso. En esta sección se ilustran los usos más frecuentes del SIP en los cuales el SER puede ser fácilmente integrado y conectado a componentes SIP como softphones, harphones, puertas enlace a la red telefónica pública conmutada y otros dispositivos.

- **Valor agregado para servicios en los proveedores de Internet**. Para atraer clientela los proveedores de Internet frecuentemente ofrecen aplicaciones a través de las redes IP, también llamadas contenidos. Estos proveedores pueden convenientemente ofrecer una variedad de servicios que corren en una infraestructura bastante simple. Particularmente, el desarrollo de servicios de VoIP y mensajería instantánea y residencial, son fáciles de configurar utilizando un servidor SIP y guiando a sus clientes a

utilizar el Windows Messenger. Adicional a esto, los proveedores pueden ofrecer servicios avanzados como una terminación y enlace a la red telefónica pública conmutada, lo cual significaría el manejo de llamadas y la unificación de mensajes, todo utilizando la misma infraestructura.

- **PC2Phone**. Los proveedores de servicios de telefonía por Internet ofrecen la capacidad de interconectar usuarios telefónicos utilizando teléfonos de software o ampliaciones hacia la red telefónica pública conmutada; particularmente con las llamadas de larga distancia internacional. Esto conlleva a un sustancial ahorro de dinero el cual puede ser alcanzado gracias al enrutamiento de las llamadas de voz a través el Internet.

- **Reemplazo de los PBX**. Reemplazar un PBX [42]tradicional en una empresa puede constituir un ahorro bastante razonable. Las empresas pueden utilizar una única infraestructura para transportar datos y voz y conectar ubicaciones distantes a través del Internet. Adicionalmente, pueden verse beneficiados por la integración de los servicios de voz y de datos.

- **Terminaciones punto a punto a la red telefónica pública conmutada**. Para reducir costos en el uso de la larga distancia y las llamadas internacionales, las compañías corporativas podrían compartir una terminación punto a punto de la red telefónica pública conmutada en sus respectivas ubicaciones. En tal escenario, dos compañías localizadas en dos ciudades pueden compartir el acceso a la red telefónica pública a través de puertas de enlace que se configuran en la otra; esto significa que si la compañía ubicada la ciudad A desea realizar llamadas a la ciudad B

[42] Private Branch Exchange. Central Telefónica Privada.

utilizaría el enlace que comparten las dos compañías para conectarse entre ellas.

7. 1. 3 Instalación y configuración del SIP Express Router.

- **Disponibilidad del SER**. SER está disponible para su descarga en la dirección ftp://ftp.berlios.de/pub/ser.

- **Instalación.**
  - **Arquitecturas soportadas**.
    - Linux/i386.
    - Linux/armv41.
    - FreeBSD/i386.
    - Solaris/sparc64.
    - NetBSD/sparc64.

  - **Requerimientos**.
    - Gcc o icc : gcc >= 2.9x; se recomienda >=3.1.
    - Bison o YACC (Berkeley YACC).
    - Flex.
    - GNU Make.
    - Sed y Tr.
    - GNU tar.
    - GNU install o BSD install.
    - Servidor de bases se satos MySQL.
    - Servidor web Apache.
    - Compatibilidad con PHP y MySQL-PHP para aplicaciones de administración a través de la web.
    - Librerías libmysqlclient.

- **Proceso de instalación**. Se debe instalar el archivo *.rpm* que se descargó del servidor FTP ejecutando la siguiente instrucción en la consola del Linux *root@localhost>rpm –i ser-08.xx-x.i386.rpm*. Luego de tener instalado el paquete se prosigue a iniciar el servicio con la instrucción *root@localhost> /etc/init.d/ser start*. En este momento se tiene el servicio funcionando pero con muy pocas capacidades y bajo nivel de seguridad.

- **Instalación de la utilidad Serctl**. Para este paso, se debe configurar primero la variable global SIP_DOMAIN para el nombre de dominio que se desea utilizar. Para esto hay dos formas de hacerlo: la primera, es ejecutando *root@localhost> export SIP_DOMAIN="mi_dominio.com"*. Esto conllevaría a configurar la variable temporalmente hasta que se reinicie el servicio. La otra forma es configurando la variable automáticamente para que cada vez que se inicie el servidor esté ya relacionada con el nombre del dominio. Para esto se debe editar el archivo de configuración de perfiles que está ubicado en la ruta */etc/profile* y agregar la línea *export SIP_DOMAIN="mi_dominio.com"* al final del archivo. Para el caso en que se esté utilizando otro equipo en la red para el manejo de las bases de datos de mantenimiento de sus suscriptores, la variable *SQL_HOST* se debe hacer coincidir editando el script de serctl.

- **Creación de las bases de datos para el manejo de los clientes**. Para instalar soporte de bases de datos de MySQL se necesita descargar el paquete *ser-mysql*, el cual está disponible en la misma ubicación donde se descargó el servidor SER. Este paquete contiene los scripts necesarios para crear las bases de datos requeridas y establecer permisos para el ingreso al servidor de bases de datos. Se recomienda instalar una versión reciente del servidor MySQL ya que se podrían presentar problemas con la sintaxis y

esto podría conllevar a errores en la configuración de los permisos para acceder a las bases de datos. Este servidor puede ser descargado gratuitamente de la dirección http://www.mysql.com. Teniendo instalado y corriendo el servidor de bases de datos se debe ejecutar el comando */usr/sbin/ser_mysql.sh* y si no aparecen errores los permisos y las bases de datos necesarias ya habrán sido instaladas.

- **Configuración del SER para el caso en particular**. Ahora que se tiene trabajando la base de datos de MySQL, se necesita modificar el archivo de configuración del SER ubicado en la extensión */etc/ser/ser.cfg*. Los siguientes cambios deben ser realizados.

  Para permitir la compatibilidad con las bases de datos ya creadas se debe cargar el módulo que lo permite, esto se realiza añadiendo la línea *loadmodule "/usr /lib /ser /modules /mysql.so"*. A continuación se necesita que el SER utilice las bases de datos para registrar los cambios periódicamente en ellas en vez de sólo cargarlos en la memoria cache. Se debe eliminar la línea *modparam ("usrloc", "db_mode", 0)* y cambiarla por la línea *modparam ("usrloc", "db_mode", 2)*. La variable *db_mode* se puede configurar de tres maneras.

  - **Modo 0.** Deshabilita la escritura en la base de datos. La información de contactos no será preservada si el servidor se reinicia.

  - **Modo 1.** Escribe todos los cambios en la base de datos inmediatamente, es decir, la información de contactos es almacenada en la base de datos tan pronto se genera. Esto puede minimizar los

recursos del servidor y crear una respuesta lenta a los clientes cuando se conecten.

- **Modo 2**. Periódicamente se actualiza la base de datos con la información de los contactos almacenada en la memoria cache.

Para permitir la autentificación se necesita añadir las líneas encargadas de esto las cuales son.

- loadmodule "/usr/lib/ser/modules/auth.so".
- loadmodule "/usr/lib/ser/modules/auth_db.so".

Se tiene la opción de guardar las contraseñas en la base de datos en texto plano. Esto permite la recuperación de estas y facilita la configuración y las pruebas al principio de la instalación. Se deben añadir las líneas siguientes.

- modparam ("auth_db", "calculate_ha1", yes)
- modparam ("auth_db", "password_column", "password").

Las dos instrucciones anteriores funcionan en conjunto. La primera le indica al servidor que debe calcular el resumen criptográfico basado en el nombre de usuario, la contraseña y el dominio. La segunda instrucción le dice servidor donde debe buscar las contraseñas en texto plano en la base de datos.

Finalmente se debe actualizar la sección del enrutamiento para reconocer el dominio, así pues, se debe reemplazar la sentencia *(uri=="myself")* por *(uri=~"midominio.com")*. Al tener estos cambios ya realizados en el archivo de configuración y se debe reiniciar el servicio con la instrucción *root@localhost> /etc/rc.d/init.d/ser restart*.

- **Añadir nuevos usuarios con la herramienta serctl**. Si no se tiene una herramienta **web** embebida en el sistema que maneje el ingreso de nuevos usuarios y la suscripción de los mismos se debe utilizar la herramienta **serctl** para ello.

  Si se quiere añadir el usuario "andres" con la contraseña "qwerty" y la dirección de correo electrónico "andres@mydomain.com" se debe ejecutar el comando *root@localhost> serctl add andres qwerty andres@mydomain.com* en la línea de comandos de la consola de Linux.

- **Examinar la memoria cache con la herramienta serctl**. Para probar si el servidor está registrando los usuarios que están conectados a él, la herramienta *serctl* es muy útil para extraer información de los usuarios registrados de la memoria cache. Para ello se debe ejecutar el comando *root@localhost> serctl ul show* el cual da como resultado una lista de los usuarios registrados en el momento. Un ejemplo de lo que retorna este comando se muestra en la figura 36.

Figura 36. Respuesta del comando *serctl ul show*.

```
===Domain list===
---Domain---
name : 'location'
size : 512
table: 0x402ee6d0
d_ll {
    n    : 2
    first: 0x402f1a74
    last : 0x402f089c
}
lock : 0

...Record(0x402f1a74)...
domain: 'location'
aor   : 'test'
~~~Contact(0x402f708c)~~~
domain : 'location'
aor    : 'test'
Contact: 'sip:test@192.168.0.100:5060'
Expires: 2501
q      :       0.00
Call-ID: '000a8a93-d4660017-4571a6cd-658ac1bf@192.168.0.100'
CSeq   : 101
State  : CS_SYNC
next   : (nil)
prev   : (nil)
~~~/Contact~~~~
.../Record...
...Record(0x402f089c)...
domain: 'location'
aor   : 'joe'
~~~Contact(0x402f0924)~~~
domain : 'location'
aor    : 'joe'
Contact: 'sip:192.168.0.101:14354'
Expires: 432
q      :       0.00
Call-ID: 'e8d93059-e46e-4fd9-958b-ccb36a1cf245@192.168.0.101'
CSeq   : 11
State  : CS_SYNC
next   : (nil)
prev   : (nil)
~~~/Contact~~~~
.../Record...
---/Domain---
===/Domain list===
```

- **Examinar el estado del servidor**. Se pueden utilizar dos comandos para revisar el estado de funcionamiento del servidor. El primero es *serctl ps* el

cual retorna una lista de todos los procesos relacionados con el servidor SER, las direcciones IP y el puerto por donde se está esperando conexión (Figura 34).

Figura 37. Respuesta del comando *serctl ps*.

```
[root@gateway /root]# serctl ps
0       31029   attendant
1       31033   receiver child=0 sock=0 @ 127.0.0.1::5060
2       31034   receiver child=1 sock=0 @ 127.0.0.1::5060
3       31035   receiver child=2 sock=0 @ 127.0.0.1::5060
4       31036   receiver child=3 sock=0 @ 127.0.0.1::5060
5       31037   receiver child=0 sock=1 @ 192.168.0.1::5060
6       31038   receiver child=1 sock=1 @ 192.168.0.1::5060
7       31039   receiver child=2 sock=1 @ 192.168.0.1::5060
8       31040   receiver child=3 sock=1 @ 192.168.0.1::5060
9       31049   fifo server
10      31072   timer
```

El segundo comando es el *serctl monitor* el cual muestra la versión del servidor, el tiempo de operación, transacciones pendientes y completadas, y el número de respuestas del servidor (Figura 35).

Figura 38. Respuesta del comando *serctl monitor*.

```
[cycle #: 1; if constant make sure server lives and fifo is on]
Up Since: Mon Dec  2 21:21:11 2003
Up time: 132711 [sec]
Transaction Statistics
Current: 0 (2 waiting) Total: 46 (0 local)
Replied localy: 37
Completion status 6xx: 0, 5xx: 0, 4xx: 23, 3xx: 0,2xx: 22
Stateless Server Statistics
200: 101 202: 0 2xx: 0
300: 0 301: 0 302: 0 3xx: 0
400: 0 401: 0 403: 0 404: 132 407: 0 408: 0 483: 1 4xx: 0
500: 0 5xx: 0
6xx: 0
xxx: 0
failures: 0
UsrLoc Stats
Domain Registered Expired
```

7. 1. 4 Problemas y limitaciones. Como uno de los objetivos de diseño que acompañan al SIP es descentralizar la inteligencia en el manejo de las comunicaciones, un tema básico es que los clientes puedan comunicarse directamente unos con otros. El problema de muchos clientes es que se encuentran o detrás de un firewall o detrás de un espacio de direcciones limitado por un NAT. En este caso, cuando un cliente se registra en un servidor SIP, su dirección IP no puede ser accesible públicamente.

- **NAT Traversal**. Hay un par de opciones que se pueden convertir en la solución para el problema que un espacio de direcciones limitadas por un NAT puede introducir. Una opción es que algunos proveedores de clientes integran a sus productos opciones para permitir al usuario identificar la dirección IP que su teléfono parece tener a nivel público. Este es un acercamiento simple, pero presume que la persona que está instalando y configurando el dispositivo conoce su dirección IP y eso si ésta no cambia. Fabricantes como Cisco Systems han desarrollado esta capacidad para sus teléfonos SIP de la serie 79xx. Otra solución que está funcionando satisfactoriamente es un proceso llamado STUN (Simple Traversal of UDP trough NAT). Un cliente equipado con esta tecnología es configurado para mandar paquetes de inspección a un servidor conocido públicamente. Este servidor le responde al cliente que se está comunicando con él, con la dirección IP aparente en el exterior del límite del NAT, esta dirección es utilizada por el cliente para registrarse en un servidor SIP.

- **Firewalls**. Los clientes también presentan un reto interesante para configurar un Firewall. Durante el proceso de registro, al cliente se le asigna un puerto UDP en un rango entre 16348 y 32768. El administrador del Firewall posiblemente no lo configure para permitir la transferencia a través de todos estos puertos. Aquí es cuando el concepto del protocolo de control

de Firewall (FCP) entra en juego. La idea de diseño es que cuando un cliente SIP se registre, un agente FCP inserta dinámicamente una nueva regla en las políticas del Firewall, permitiendo que el cliente participe en una sesión SIP.

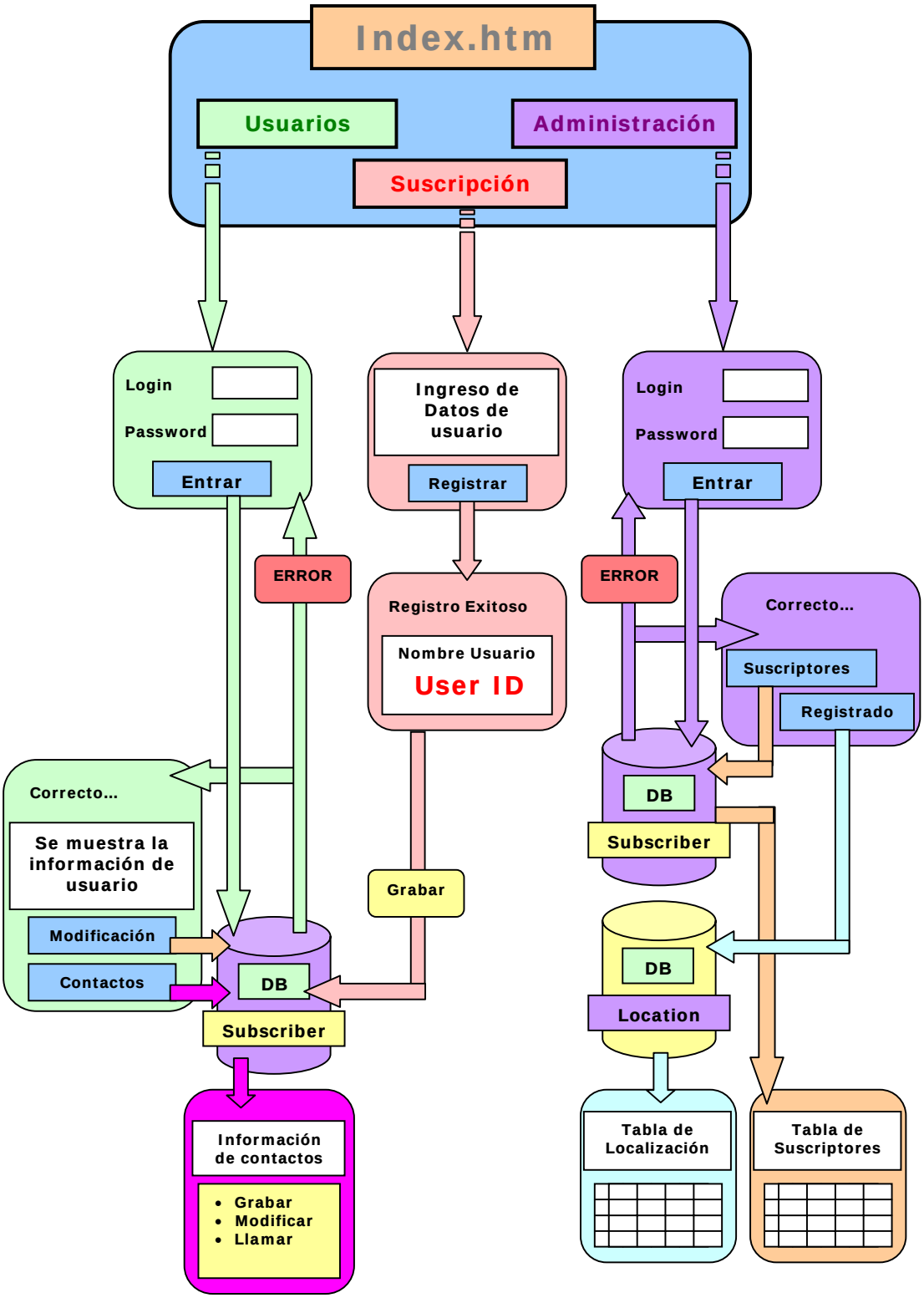
7. 2 SERVICIO WEB

7. 2. 1 Descripción y justificación. Para diseñar un sistema que preste un servicio eficiente a usuarios de todos los niveles hay un aspecto muy importante que se debe tener en cuenta, la accesibilidad. Debido a esto se decidió extender el alcance del proyecto hacia el desarrollo de un servicio web dedicado e interconectado al servicio de voz sobre IP. El diseño de este servicio debe estar basado en unas directivas de gestión de sistemas avanzados en telemática, esto significa que debe permitir un acceso seguro a la información personal de los usuarios. También el servicio debe tener directivas y herramientas para que sus administradores puedan lograr eficientemente un diagnóstico del sistema general y les permita tener control privilegiado sobre los recursos, cuentas y transacciones que se realicen a través del servicio de voz sobre IP.

7. 2. 2 Esquema general y diagrama de operación. El servicio web que complementa el sistema de voz sobre IP posee tres secciones generales: Entrada de usuarios, entrada de suscriptores y entrada de administración. Cada una de estas estapas se muestra en la siguiente figura y se explicara a continuación.

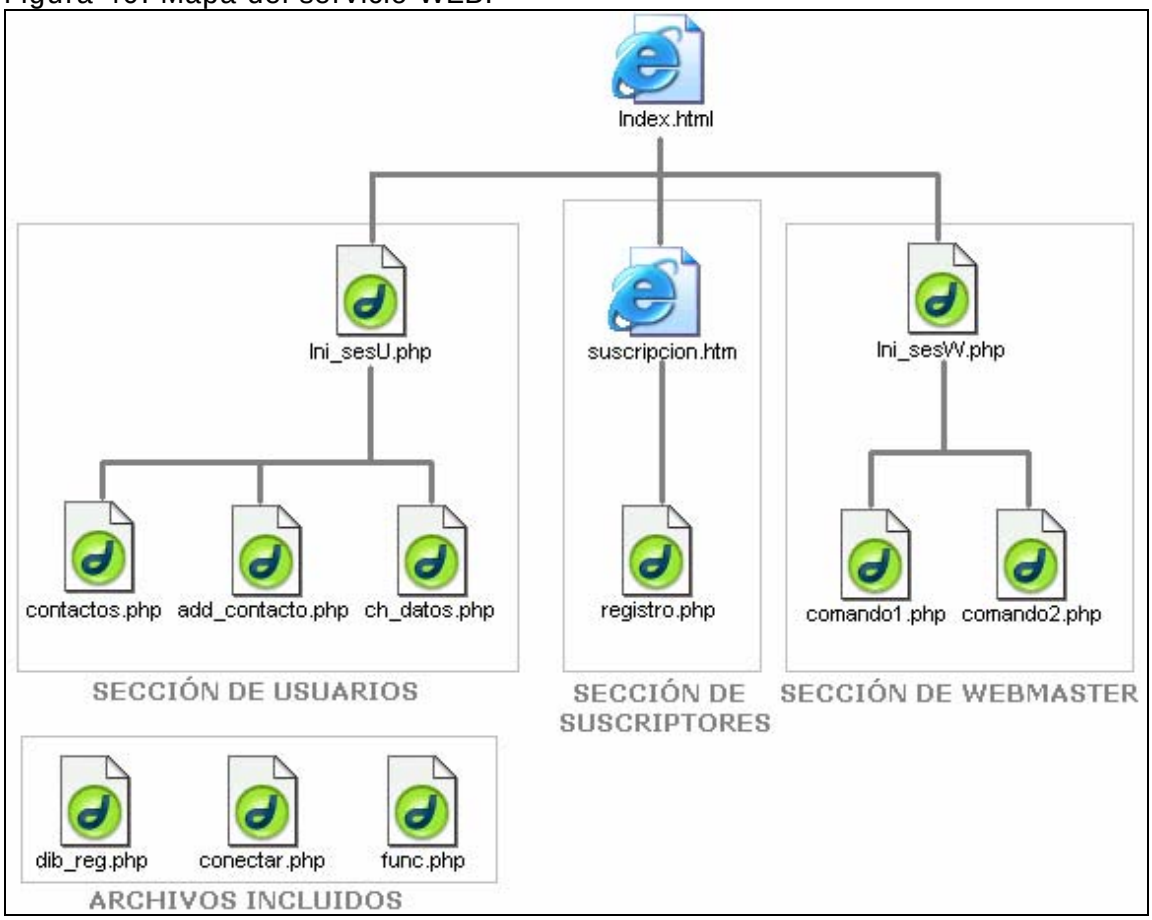
- Mapa y diagrama del servicio WEB.

Figura 39. Diagrama del servicio WEB.



En esta sección se describe gráficamente el diagrama del servicio web (Figura 39) y el mapa del servicio WEB del sistema de voz sobre IP (Figura 40). Esta página web fue desarrollada con los lenguajes PHP y HTML. Se utilizó el pre-procesador de hipertexto PHP ya que además de ser un lenguaje de uso gratuito, es una herramienta con una poderosa arquitectura en cuestiones de seguridad además de tener una amplia variedad de funciones de fácil manejo para lograr una implementación robusta y así poder establecer conexiones con el servidor bases de datos de MySQL que sirve al SIP Express Router.

Figura 40. Mapa del servicio WEB.



- Descripción detallada de los archivos *.php* y *.html* más importantes del servicio WEB.

  - Index.htm: Consiste básicamente en información general sobre el proyecto. Es la página de presentación y mediante esta se puede acceder a las tres secciones principales del servicio web: suscripción, usuarios y entrada de administrador. A continuación se describirá cada uno de los archivos web que contiene cada sección.

  - Sección de suscripción: Una parte importante del sistema es poder suscribirse al servicio. Mediante esta sección el usuario queda registrado en la base de datos de MySQL que utiliza el SER para comprobar los datos enviados por el usuario agente a la hora del registro en el servicio de ubicación temporal.

    - Suscripción.htm: Básicamente en este documento HTTP hay una forma en donde el usuario escribe sus datos como nombres, apellidos, e-mail, y dos casillas para la contraseña de la cuenta las cuales deben coincidir y estar entre 4-14 caracteres. Esta documento mediante el método POST envía toda la información del usuario al archivo HTTP registro.php.

    - Registro.php: En este documento se realiza la validación de los datos enviados por el usuario en la cual se revisa que las contraseñas digitadas coincidan mutuamente y que no falte ningún dato, además de validar el formato de la dirección de correo. Si hay algún problema en la validación anterior no se precede a la incorporación

del usuario en el servicio, en vez, se le indica que información debe corregir o incluir. Si la validación de los datos del nuevo usuario no arroja excepciones, entonces se procede a insertar al usuario a la base de datos. En este caso se utilizaron las funciones que posee el PHP para conexión, inserción y búsqueda en bases de datos MySQL mediante comandos SQL. Primero que todo se debe conectar a la base de datos deseada, esto se hace mediante el código siguiente:

```
<?php
        $link=mysql_connect("localhost","root","XXXXXXXX");
        $db="ser";
?>
```

Luego se reciben los datos y se insertan en la base de datos en la tabla “subscriber” mediante el siguiente código:

```
$sql="select * from subscriber";
$res=send_sql($db,$sql);
$cant=mysql_num_rows($res);
$user=$puntero + $cant;
$sql="insert into subscriber (phone, datetime_created,_ domain, ha1b, ha1, phplib_id, username, password,_ first_name, last_name, email_address) values ('$user',_ '$fecha', 'dominio.com', '$ha1b', '$php_lib', '$php_lib',_ '$user', '$password1', '$nombre', '$apellido', '$e_mail')";
```

Es este código se encuentra una constante llamada $puntero la cual se usa para generar un número telefónico para cada usuario el cual

se le muestra junto con su contraseña en texto plano luego de ejecutarse el código. En este momento el usuario ya esta suscrito al servicio y puede hacer uso del mismo.

- Sección de Usuarios: En esta sección el usuario puede ver su información personal, cambiar su contraseña, ver las páginas blancas, añadir y ver contactos.

  - Ini_sesU.php: En este momento la seguridad es importante por lo tanto se editó el documento "php.ini" para permitir el uso de sesiones y para que las variables nunca sean globales haciendo la variable register_globals = "Off". Lo anterior se hizo paso a paso según las recomendaciones del PHP Group las cuales se encuentran en el manual de PHP de libre distribución en el Internet. Otro aspecto importante es que los archivos de sesión deben ser únicos por cada usuario para que el servidor no se llene de basura al crearse una cookie por cada vez que un usuario acceda al servicio web. En este archivo de sesión único por usuario se carga toda la información del usuario necesaria para cualquier proceso dentro del servicio al iniciarse esta, lo anterior para hacer más eficiente el sistema evitando conexiones innecesarias a la base de datos cada vez que se necesite información. Lo anterior se logra con el siguiente código:

```
$username=$_SERVER['PHP_AUTH_USER'];
$password=$_SERVER['PHP_AUTH_PW'];
$sql="select * from subscriber where username = '$username'";
$res=send_sql($db,$sql);
$row=mysql_fetch_array($res);
```

```
if ($row['password']==$password and $username!=NULL)
  {
   session_id(resumen_cript($usename,$password));
    session_start();
    header("Cache-control: private");
    $auth_u='OK';
    $_SESSION['perms']='user';
    $_SESSION['nombre']=$row['first_name'];
    $_SESSION['apellido']=$row['last_name'];
    $_SESSION['e_mail']=$row['email_address'];
  }
  else
  {
   $auth_u='Fail';
  }


<?php
    function resumen_cript($username,$password)
    {
    $len1=strlen($password);
    $len2=strlen($username);
    $len=$len1+$len2;
    $cadena=str_pad($username,$len,$password);
    $resumen=sha1($cadena);
    return $resumen;
    }
?>
```

La línea *session_id(resumen_cript($usename,$password))* crea una sesión única cuyo identificador es un número hexagesimal de 40

nibbles único para cada combinación de contraseña y número telefónico. La función *resumen_cript()* realiza una concatenación de las cadenas de número telefónico y nombre de usuario para luego aplicarle a esta el algoritmo sha1($cadena) el cual es el Algoritmo de Hash Seguro US 1. Después de este proceso se abre la sesión con la línea *session_start()* para luego introducir los datos del usuario que residen en la tabla “subscriber” en el cookie de la sesión.

En esta sección de usuarios se puede ver contactos, añadirlos y cambiar los datos personales del usuario que se loggea.

- Ini_sesU.php: La seguridad de esta sección es parecida a la de la sección de usuarios solo que la entrada depende además del permiso que posea el usuario en la taba “subscribers” en el campo “perms” el cual debe tener la cadena “admin”.

  En esta sección el(los) administrador(es) del servicio puede(n) ver el comportamiento del sistema mediante dos comandos SQL[43]:

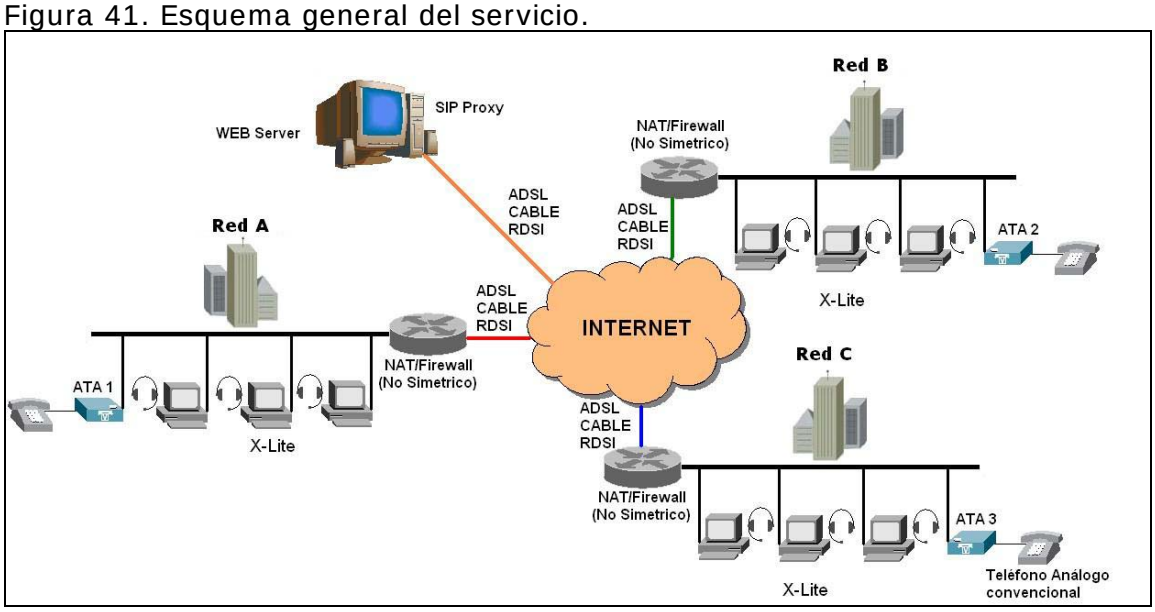
  - "select username, domain, password, first_name, last_name, phone, email_address, datetime_created from subscriber": Este comando revisa todos los datos de los suscriptores.

[43] Lenguaje de sentencias de pregunta que permite establecer consultas en bases de datos locales o remotas.

- "select * from location": Este comando revisa la tabla del servicio de ubicación el cual muestra a los usuarios en línea con su dirección y puerto IP.

7. 3 DESARROLLO Y DISEÑO DEL SERVICIO

Figura 41. Esquema general del servicio.



7. 3. 1 Esquema general. La gran ventaja de un servicio de voz sobre IP es su versatilidad y relativa facilidad de implementación en cuanto a infraestructura e ínterconectividad. Primero que todo, para la implementación de este es necesario contar con una red que soporte el protocolo TCP/IP, por ejemplo la red interna de la Universidad Autónoma de Occidente. Es necesario también contar con puntos acceso a la red por medio de un cableado estructurado. Teniendo esta infraestructura se prosigue a instalar en un computador el servicio de voz sobre IP el cual es la conjunción de cuatro diferentes sistemas; el servidor SIP proxy, el servidor de registro SIP, el

servidor web y el servidor MySQL para el manejo de bases de datos. Al tener esto instalado, configurado y funcionando conjuntamente se prosigue sencillamente a configurar los clientes del servicio. Estos clientes pueden ser teléfonos SIP, adaptadores SIP de teléfonos análogos o teléfonos de software. El esquema general se muestra en la figura 41.

7. 3. 2 Problemas, dificultades y soluciones. Es importante tener en cuenta ciertos aspectos para un correcto funcionamiento del servicio. La mayoría de los problemas que se presentaron en el montaje fueron básicamente de dos naturalezas: configuración del software y configuración de los clientes. A continuación se describirán los inconvenientes que se tuvieron en cada una de estas áreas.

- **Problemas de instalación del software y su respectiva solución práctica**.
  - El servidor de bases de datos Mysql no corría debido a que el socket *MySQL.sock* no existía.
    - Solución. Algo importante en la instalación del servidor MySQL, que no es mencionado en el documento de instalación del mismo, es el hecho de que al instalar el servidor en Linux, el socket [44]es creado en la siguiente inicialización del sistema, por ende para que este se cree se debe reiniciar el sistema completamente así el error no vuelve a salir.

  - Al intentar correr el servicio relacionado con el servidor SER se detectó un error en el archivo de configuración *ser.cfg*.

- Solución. Este error significa que el archivo de configuración *ser.cfg* tiene un error de sintaxis, probablemente introducido por la persona que lo editó. Para evitar esto se debe tener especial cuidado al hacer los cambios respectivos descritos anteriormente, pero si no se encuentra solución evidente, se debe proseguir a parar el servicio y reinstalar el RPM[45] que contiene el SER.

➢ Al hacerse peticiones al servicio web desde una estación remota, este no respondía y generaba entonces un error del tipo *404 Not Found* y se visualizaba en el navegador el mensaje "*no se puede mostrar la página*".

- Solución 1. Se debe revisar que la directiva *DocumentRoot* en el archivo de configuración *httpd.conf* del servidor Apache contenga la ruta correcta de la ubicación de la página.

- Solución 2. La mayoría de veces el usuario inexperto al instalar el sistema operativo Linux ignora la configuración del Firewall residente. Esta configuración es importante ya que al ser ignorada se crean reglas de seguridad que para nada concuerdan con la que el usuario desea para sus servicios, por ejemplo el servicio Web. Para configurar el permiso para que usuarios externos envíen peticiones http al servidor se debe ingresar esta regla al Firewall por medio del comando *setup* digitado en consola. Al ejecutar el comando *setup* se muestra un pantallazo con las opciones para configurar distintas características del sistema; aquí se escoge la opción *Firewall*

[44] Puerto lógico.
[45] Paquete de auto extracción para el sistema operativo Linux.

configuration. Al estar en la configuración del Firewall, se habilita la opción de *http* y se habilita el puerto *5060*; luego se graba este cambio.

- Solución 3 Se debe asegurar que el servicio httpd (Apache Web Server) este corriendo correctamente mediante el comando *root@localhost> httpd status.* Si el servicio no esta corriendo se debe correr mediante el comando *root@localhost> httpd start*.

❖ **Problemas debidos a la configuración de los clientes**.

- El cliente no envía peticiones de registro al servidor.
  - Solución 1. Para solucionar esto se debe activar la característica *SIP send registration* en el dispositivo SIP asociado al problema.

  - Solución 2. Se debe revisar que la dirección IP del dispositivo SIP es diferente de 0.0.0.0 y además no debe tener la misma dirección IP de otro dispositivo ya que esto origina un conflicto.

- El cliente envía peticiones de registro al servidor pero recibe como respuesta a un *408 Not Authorized*.
  - Solución. Se debe revisar que el servidor, la contraseña y el nombre de usuario sean correctos y coincidan con la información suministrada por el servidor web en el momento de la suscripción al servicio.

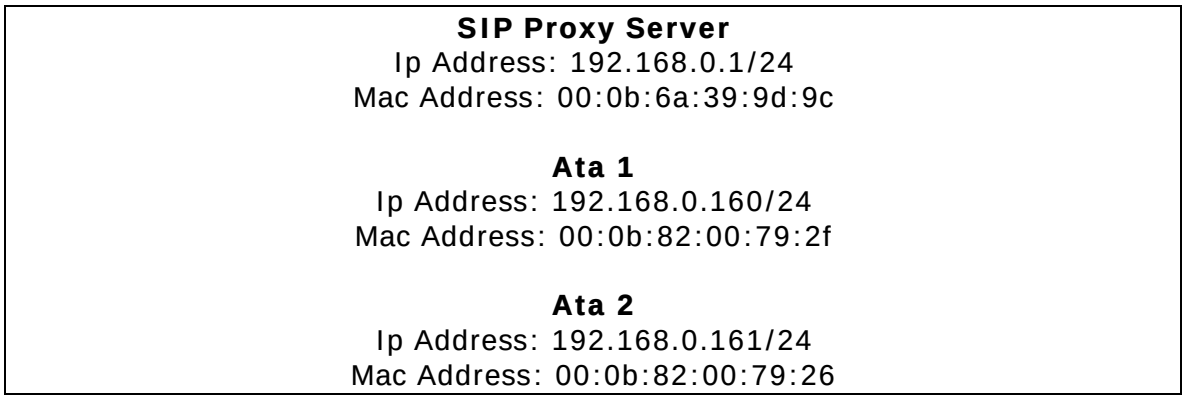
- El cliente se registra correctamente y al llamar a otro cliente la información multimedia de la sesión es nula o se transmite en un solo sentido.

  En este caso las soluciones dependerán de la red en donde se encuentre el usuario SIP ya que si este no conoce las directivas de seguridad y las limitaciones de servicios impuestas por el administrador de la red en las tablas de acceso extendidas del NAT/Firewall, le es imposible solucionar este problema. Para el caso que se quiera acceder al servicio desde una red corporativa, la responsabilidad de la prestación del mismo depende de los administradores de la red, inclusive se podría necesitar la implementación de nueva infraestructura (Servidores TURN y STUN). En la sección 6. 12 de este documento, "*Escenarios y soluciones para aplicaciones SIP que corren dentro de un NAT/Firewall*", se desarrollara este tema de manera más detallada.

7. 3. 3 Pruebas y resultados. Existe una gran diversidad de situaciones que se pueden presentar en una sesión a través del protocolo SIP, desde el registro hasta la desconexión de los usuarios.

Para este análisis se uso el Software analizador de Redes ETHEREAL, el cual es perfectamente compatible en el ambiente Linux y el Windows. Los elementos que conforman la red local que se implementó para analizar algunos de los casos que se pueden presentar se describen en la figura 42.

Figura 42. Elementos de prueba.



Estos datos de las direcciones Mac y las direcciones IP son obtenidas a través de peticiones ARP con tramas Broadcast.

A continuación se presentaran algunas de las situaciones más comunes haciendo énfasis en los siguientes niveles de la especificación OSI:

- Nivel de Enlace.
- Nivel de Red.
- Nivel de Transporte.
- Nivel de Sesión.

- **Situación 1. Registro exitoso de los usuarios**.

  Si los Ata's (En general todos los dispositivos que se pueden usar) se encuentran configurados correctamente, si el servidor SIP Proxy esta activo y si este mismo se encuentra al alcance del usuario, entonces se hará el registro satisfactoriamente de cada uno de los usuarios que cumplan estas condiciones en el Servidor SIP.

- Petición de registro del Ata (3304076) al SIP Proxy Server:

```
Ethernet II
      Destination: 00:0b:6a:39:9d:9c (Asiarock_39:9d:9c)
      Source: 00:0b:82:00:79:2f (Grandstr_00:79:2f)
      Type: IP (0x0800)
Internet Protocol
      Version: 4
      Header length: 20 bytes
      Differentiated Services Field: 0x00 (DSCP 0x00: Default;
      ECN: 0x00)
      Total Length: 706
      Identification: 0x47f3 (18419)
      Flags: 0x00
      Fragment offset: 0
      Time to live: 250
      Protocol: UDP (0x11)
      Header checksum: 0xf445 (correct)
      Source: 192.168.0.160 (192.168.0.160)
      Destination: 192.168.0.1 (192.168.0.1)
User Datagram Protocol
      Source port: 5060 (5060)
      Destination port: 5060 (5060) (*1)
      Length: 686
      Checksum: 0x5009 (correct)
Session Initiation Protocol
      Request-Line: REGISTER sip:prosip.com SIP/2.0
            Method: REGISTER (*2)
            Resent Packet: False
      Message Header
            Via: SIP/2.0/UDP
            192.168.0.160;branch=z9hG4bK98341d205766d2f4
```

```
From:
   SIP from address: "Andres Parra"
   <sip:3304076@prosip.com;user=phone>
   SIP tag: c2ab580eb79b1f9b
To: <sip:3304076@prosip.com;user=phone>
Contact: <sip:3304076@192.168.0.160;user=phone>
Authorization:
   DIGEST username="3304076",
   realm="prosip.com",
   algorithm=MD5,
   uri="sip:prosip.com",
   nonce="40a817c894545ef95d0c8b45e0ea40401d29922b
   ", response="ef8c6883f4eb6a57859c657a1a45ca0e"
Call-ID: b035b8343b6e899d@192.168.0.160
CSeq: 203 REGISTER
Expires: 60
User-Agent: Grandstream HT286 1.0.4.49
Max-Forwards: 70
Allow:  INVITE,ACK,CANCEL,BYE,NOTIFY,REFER,
      OPTIONS,INFO,SUBSCRIBE
Content-Length: 0
```

- Respuesta del SIP Proxy Server al Ata (3304076):

```
Ethernet II
      Destination: 00:0b:82:00:79:2f (Grandstr_00:79:2f)
      Source: 00:0b:6a:39:9d:9c (Asiarock_39:9d:9c)
Internet Protocol
      Total Length: 633
      Identification: 0x0000 (0)
      Flags: 0x04 (Don't Fragment)
```

```
      Time to live: 64
      Protocol: UDP (0x11)
      Source: 192.168.0.1 (192.168.0.1)
      Destination: 192.168.0.160 (192.168.0.160)
User Datagram Protocol
      Source port: 5060 (5060)
      Destination port: 5060 (5060)
      Length: 613
Session Initiation Protocol
      Status-Line: SIP/2.0 200 OK
            Status-Code: 200 (*3)
            Resent Packet: False
      Message Header
            Via: SIP/2.0/UDP
            192.168.0.160;branch=z9hG4bK98341d205766d2f4
            From:
               SIP from address: "Andres Parra"
               <sip:3304076@prosip.com;user=phone>
               SIP tag: c2ab580eb79b1f9b
            To: <sip:3304076@prosip.com;user=phone>;
                  tag=b27e1a1d33761e85846fc98f5f3a7e58.f6ee
            Call-ID: b035b8343b6e899d@192.168.0.160
            CSeq: 203 REGISTER
            Contact:
               <sip:3304076@192.168.0.160;
               user=phone>;
               q=0.00;
               expires=60
            Server: Sip EXpress router (0.8.12 (i386/linux))
            Content-Length: 0
```

- **Nota:** Para efectos de organización y un mejor entendimiento se suprimen los campos de la captura que son idénticos a los datos anteriores. En esta primera parte se expuso detalladamente cada uno de los campos de todo el flujo de datos para establecer una comunicación a través del protocolo SIP en una red de Área Local. De acá en adelante solo se mostraran los campos más importantes y los que presenten algún cambio. Los campos resaltados y con asterisco ***(*)*** se explican al final de cada caso.

➢ Petición de Registro del Ata (3306478) al SIP Proxy Server:

```
Ethernet II
      Destination: 00:0b:6a:39:9d:9c (192.168.0.1)
      Source: 00:0b:82:00:79:26 (192.168.0.161)
Internet Protocol
      Protocol: UDP (0x11)
      Source: 192.168.0.161 (192.168.0.161)
      Destination: 192.168.0.1 (192.168.0.1)
User Datagram Protocol
      Source port: 5060 (5060)
      Destination port: 5060 (5060) (*1)
Session Initiation Protocol
      Request-Line: REGISTER sip:prosip.com SIP/2.0
         Method: REGISTER (*2)
         Resent Packet: False
      Message Header
         Via: SIP/2.0/UDP
         192.168.0.161;branch=z9hG4bK50898316d5f7dcf8
         From:
```

```
            SIP from address: "Andres Botero"
            <sip:3306478@prosip.com;user=phone>
            SIP tag: 46427907e7f3718d
      To: <sip:3306478@prosip.com;user=phone>
      Contact: *
      Authorization:
         DIGEST username="3306478",
         realm="prosip.com",
         algorithm=MD5, uri="sip:prosip.com",
         nonce="40afe3c6853b4ece46e923301488069f52da2be0",
         response="7e6b221392941c67af1f2d270bc61561"
      Call-ID: a3f988c41d5c71ca@192.168.0.161
      CSeq: 101 REGISTER
      Expires: 0
      User-Agent: Grandstream HT286 1.0.4.50
      Max-Forwards: 70
      Allow: INVITE,ACK,CANCEL,BYE,NOTIFY,REFER,
            OPTIONS,INFO,SUBSCRIBE
      Content-Length: 0
```

- Respuesta del SIP Proxy Server al Ata (3306478):

```
Ethernet II
      Destination: 00:0b:82:00:79:26 (192.168.0.161)
      Source: 00:0b:6a:39:9d:9c (192.168.0.1)
Internet Protocol
      Protocol: UDP (0x11)
      Source: 192.168.0.1 (192.168.0.1)
      Destination: 192.168.0.161 (192.168.0.161)
User Datagram Protocol
```

```
      Source port: 5060 (5060)
      Destination port: 5060 (5060)
Session Initiation Protocol
      Status-Line: SIP/2.0 200 OK
         Status-Code: 200 (*3)
         Resent Packet: False
      Message Header
         Via: SIP/2.0/UDP
         192.168.0.161;branch=z9hG4bK50898316d5f7dcf8
         From:
               SIP from address: "Andres Botero"
               <sip:3306478@prosip.com;user=phone>
               SIP tag: 46427907e7f3718d
         To: <sip:3306478@prosip.com;user=phone>;
            tag=b27e1a1d33761e85846fc98f5f3a7e58.14d5
         Call-ID: a3f988c41d5c71ca@192.168.0.161
         CSeq: 101 REGISTER
         Server: Sip EXpress router (0.8.12 (i386/linux))
         Content-Length: 0
```

- (*1) Los Ata's esta configurados para asignar un Puerto UDP para el transporte de los datos. Si no se asigna ninguno el toma por defecto el puerto *5060* que es el puerto por defecto para el protocolo SIP.
- (*2) Para hacer la petición de registro por parte del usuario se usa el Método *Register.*
- (*3) Cuando todos los parámetros se han configurado correctamente para el registro del usuario en el SIP Proxy, el servidor retorna un comando *200 (ok)*, lo cual significa que el usuario ha sido registrado correctamente.

❖ **Situación 2. Contraseña inválida.**

En la red local uno de los usuarios tiene una contraseña de ingreso valida (3304076) y el otro no (3306478). Se puede observar que uno puede registrarse y el otro tiene el acceso denegado. A continuación se presentan las tramas con los flujos de datos presentes en este caso expuesto.

➢ Petición de registro del Ata (3306478) al SIP Proxy Server:

```
Ethernet II
      Destination: 00:0b:6a:39:9d:9c (Asiarock_39:9d:9c)
      Source: 00:0b:82:00:79:26 (Grandstr_00:79:26)
Internet Protocol
      Protocol: UDP (0x11)
      Source: 192.168.0.161 (192.168.0.161)
      Destination: 192.168.0.1 (192.168.0.1)
User Datagram Protocol
      Source port: 5060 (5060)
      Destination port: 5060 (5060)
Session Initiation Protocol
      Request-Line: REGISTER sip:prosip.com SIP/2.0
            Method: REGISTER
            Resent Packet: True (suspected resend of frame 1)
      Message Header
            Via: SIP/2.0/UDP
            192.168.0.161:5002;branch=z9hG4bK07b2d3b71c06b829
            From:
               SIP from address: "Andres Botero"
               <sip:3306478@prosip.com;user=phone>
```

```
      SIP tag: 2cdf54399046adf1
   To: <sip:3306478@prosip.com;user=phone>
   Contact: *
   Authorization:
      DIGEST username="3306478",
      realm="prosip.com",
      algorithm=MD5,
      uri="sip:prosip.com",
      nonce="40a817d95f2ced1334f8c267b395389960efd825
      ",
      response="0dcefc7ebc4fdda34f891a82ceea254f"
   Call-ID: c1a8879686480e23@192.168.0.161
   CSeq: 101 REGISTER
   Expires: 0
   User-Agent: Grandstream HT286 1.0.4.50
   Max-Forwards: 70
   Allow:  INVITE,ACK,CANCEL,BYE,NOTIFY,REFER,
         OPTIONS,INFO,SUBSCRIBE
   Content-Length: 0
```

- Respuesta del SIP Proxy Server al Ata (3306478):

```
Ethernet II
     Destination: 00:0b:82:00:79:26 (Grandstr_00:79:26)
     Source: 00:0b:6a:39:9d:9c (Asiarock_39:9d:9c)
Internet Protocol
     Protocol: UDP (0x11)
     Source: 192.168.0.1 (192.168.0.1)
     Destination: 192.168.0.161 (192.168.0.161)
User Datagram Protocol
     Source port: 5060 (5060)
```

```
     Destination port: 5060 (5060)
Session Initiation Protocol
     Status-Line: SIP/2.0 401 Unauthorized
          Status-Code: 401 (*1)
          Resent Packet: False
     Message Header
          Via: SIP/2.0/UDP
          192.168.0.161:5002;branch=z9hG4bK9c3a9177b7e4a578
          From:
             SIP from address: "Andres Botero"
             <sip:3306478@prosip.com;user=phone>
             SIP tag: 2cdf54399046adf1
          To:
          <sip:3306478@prosip.com;user=phone>;tag=b27e1a1d33
          761e85846fc98f5f3a7e58.7e23
          Call-ID: c1a8879686480e23@192.168.0.161
          CSeq: 101 REGISTER
          WWW-Authenticate:
             Digest realm="prosip.com",
             nonce="40a817d95f2ced1334f8c267b395389960efd825
             "
          Server: Sip EXpress router (0.8.12 (i386/linux))
          Content-Length: 0
```

- (*1) Si alguno de los datos de configuración del Ata han sido ingresados erróneamente, como en este caso que se ingreso incorrecta la contraseña para autentificación, el SIP Proxy Server retorna un comando *401(Unauthorized)*, lo cual significa que el usuario no ha sido autorizado para ser registrado.

❖ **Situación 3. El SIP Proxy Server se encuentra caído o inalcanzable para el usuario.**

En este ejemplo se ha bajado el servicio para que los usuarios no se puedan registrar. Si no hay servicio, los usuarios (Ata's, Softphones, Hardphones) continúan intentando registrarse periódicamente.

➢ El Ata (3304076) hace una petición de registro al igual que se ilustro anteriormente con el Método REGISTER.

```
Ethernet II
      Destination: 00:0b:6a:39:9d:9c (192.168.0.1)
      Source: 00:0b:82:00:79:2f (192.168.0.160)
Internet Protocol
      Protocol: UDP (0x11)
      Source: 192.168.0.160 (192.168.0.160)
      Destination: 192.168.0.1 (192.168.0.1)
User Datagram Protocol
      Source port: 5060 (5060)
      Destination port: 5060 (5060)
Session Initiation Protocol
      Request-Line: REGISTER sip:prosip.com SIP/2.0
         Method: REGISTER
         Resent Packet: False
```

Como no se encuentra el servidor habilitado entonces el host al cual se le envía la petición de registro retorna una respuesta de error a través del *Protocolo de Mensajes de Control de Internet (ICMP).* Este mensaje

indica que el destino es inválido y retorna un mensaje de *Unreachable* de la forma que se indica a continuación. Las tramas enviadas son retornadas idénticamente desde el Internet Protocol hasta el Sesion Initiation Protocol.

```
Ethernet II
      Destination: 00:0b:82:00:79:2f (192.168.0.160)
      Source: 00:0b:6a:39:9d:9c (192.168.0.1)
Internet Protocol
      Protocol: ICMP (0x01)
      Source: 192.168.0.1 (192.168.0.1)
      Destination: 192.168.0.160 (192.168.0.160)
Internet Control Message Protocol
      Type: 3 (Destination unreachable)
      Code: 3 (Port unreachable)
      Checksum: 0x80c6 (correct)
      Internet Protocol …
      User Datagram Protocol …
      Session Initiation Protocol …
```

- El Ata (3306478) hace una petición de registro al igual que se ilustro anteriormente con el Método *Register.*

```
Ethernet II
      Destination: 00:0b:6a:39:9d:9c (192.168.0.1)
      Source: 00:0b:82:00:79:26 (192.168.0.161)
Internet Protocol
      Source: 192.168.0.161 (192.168.0.161)
      Destination: 192.168.0.1 (192.168.0.1)
```

User Datagram Protocol
Source port: 5060 (5060)
Destination port: 5060 (5060)
Session Initiation Protocol
Request-Line: REGISTER sip:prosip.com SIP/2.0
Method: ***REGISTER***
Resent Packet: False

Como no se encuentra el servidor habilitado entonces el host al cual se le envía la petición de registro retorna una respuesta de error a través del *Protocolo de Mensajes de Control de Internet (ICMP).* Este mensaje indica que el destino es inválido y retorna un mensaje de *Unreachable* de la forma que se indica a continuación. Las tramas enviadas son retornadas idénticamente desde el Internet Protocol hasta el Sesion Initiation Protocol.

Ethernet II
Destination: 00:0b:82:00:79:26 (192.168.0.161)
Source: 00:0b:6a:39:9d:9c (192.168.0.1)
Internet Protocol
Source: 192.168.0.1 (192.168.0.1)
Destination: 192.168.0.161 (192.168.0.161)
Internet Control Message Protocol
Type: ***3 (Destination unreachable)***
Code: ***3 (Port unreachable)***
Checksum: 0x80cd (correct)
Internet Protocol
User Datagram Protocol
Session Initiation Protocol

❖ **Situación 4. El usuario intenta registrarse con un Username inválido**.

En este ejemplo se ha configurado el Ata (3306478) con un Username (Nombre de Usuario) que no esta registrado en la base de datos del SER. Por consiguiente lo que se espera que es que el SIP Proxy Server rechace la petición de registro como se muestra a continuación.

- El Ata (3306478) envía una Petición de Registro al SIP Proxy Server al igual que en los anteriores casos.

```
Ethernet II
      Destination: 00:0b:6a:39:9d:9c (192.168.0.1)
      Source: 00:0b:82:00:79:26 (192.168.0.161)
Internet Protocol
      Source: 192.168.0.161 (192.168.0.161)
      Destination: 192.168.0.1 (192.168.0.1)
User Datagram Protocol
      Source port: 5060 (5060)
      Destination port: 5060 (5060)
Session Initiation Protocol
      Request-Line: REGISTER sip:prosip.com SIP/2.0
         Method: REGISTER
         Resent Packet: False
      Message Header
         Via: SIP/2.0/UDP
         192.168.0.161;branch=z9hG4bK75e42bc0e2c4948f
         From:
```

```
      SIP from address: "Andres Botero"
      <sip:3306479@prosip.com (*1);user=phone>
      SIP tag: 642c800c018b4341
   To: <sip:3306479@prosip.com (*1);user=phone>
   Contact: *
   Authorization:
      DIGEST username="3306479" (*1),
      realm="prosip.com",
      algorithm=MD5,
      uri="sip:prosip.com",
      nonce="40afe825fa476bc0f932335f56d37deaf2a5fa0e",
      response="566c5101867ce0fb0e33fc1403711c73"
   Call-ID: 733468e91e55a14f@192.168.0.161
   CSeq: 100 REGISTER
   Expires: 0
   User-Agent: Grandstream HT286 1.0.4.50
   Max-Forwards: 70
   Allow: INVITE,ACK,CANCEL,BYE,NOTIFY,REFER,
        OPTIONS,INFO,SUBSCRIBE
   Content-Length: 0
```

- El SIP Proxy Server retorna el códogo *401 (Unauthorized)* denegando la petición de registro a este usuario.

```
Ethernet II
     Destination: 00:0b:82:00:79:26 (192.168.0.161)
     Source: 00:0b:6a:39:9d:9c (192.168.0.1)
Internet Protocol
     Source: 192.168.0.1 (192.168.0.1)
     Destination: 192.168.0.161 (192.168.0.161)
User Datagram Protocol
```

```
      Source port: 5060 (5060)
      Destination port: 5060 (5060)
Session Initiation Protocol
      Status-Line: SIP/2.0 401 Unauthorized
         Status-Code: 401 (*2)
         Resent Packet: False
      Message Header
         Via: SIP/2.0/UDP
         192.168.0.161;branch=z9hG4bK75e42bc0e2c4948f
         From:
            SIP from address: "Andres Botero"
            <sip:3306479@prosip.com;user=phone>
               SIP tag: 642c800c018b4341
         To:
         <sip:3306479@prosip.com;user=phone>;tag=b27e1a1d33761
         e85846fc98f5f3a7e58.b629
         Call-ID: 733468e91e55a14f@192.168.0.161
         CSeq: 100 REGISTER
         WWW-Authenticate:
            Digest realm="prosip.com",
            nonce="40afe825fa476bc0f932335f56d37deaf2a5fa0e"
         Server: Sip EXpress router (0.8.12 (i386/linux))
         Content-Length: 0
```

- (*1) El usuario con Username = “3306479” no existe en la base del SER. Por esto no se puede registrar.

- (*2) El SIP Proxy retorna el código 401 que indica que el usuario “3306479” no es autorizado y por lo tanto no puede registrarse.

❖ **Situación 5. Establecimiento de una conversación**.

En este caso los usuarios "3304076" y "3306478" se encuentran Registrados correctamente en el SIP Proxy. El usuario "*3304076*" hace una invitación a conversación al usuario "*3306478*". A continuación se ilustrara todo el proceso desde la Invitación hasta el fin de la conversación.

Nota: Se omiten los datos pertenecientes a los niveles de enlace, red (excepto las direcciones de Fuente y Destino) y transporte para un mejor enfoque en la parte que interesa para esta situación que es el nivel de Sesión. Estos campos son idénticos a los ilustrados en los casos anteriores y por eso algunos llevan tres puntos***(…)***.

- Invitación del usuario "*3304076*" con el Ata 1 al usuario "*3306478*" con el Ata 2 a través del SIP Proxy. Este envía toda la descripción de la sesión por medio del Protocolo de Descripción de Sesión *SDP.*

```
Internet Protocol
     Source: 192.168.0.160 (192.168.0.160)
     Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
     Request-Line: INVITE sip:3306478@prosip.com;user=phone
     SIP/2.0
        Method: INVITE
        Resent Packet: False
     Message Header
        Via: SIP/2.0/UDP
        192.168.0.160;branch=z9hG4bK506b1fd57eadbfc6
```

From:
SIP from address: "Andres Parra"
<sip:***3304076***@prosip.com;user=phone>
SIP tag: 18b85c51d64ea7ef
To: <sip:***3306478***@prosip.com;user=phone>
Contact: <sip:3304076@192.168.0.160;user=phone>
Call-ID: 7818bc8158c868ad@192.168.0.160
CSeq: 12775 ***INVITE***
User-Agent: Grandstream HT286 1.0.4.49
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 202
Message body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator
Owner Username: 3304076
Session ID: 8000
Session Version: 8000
Owner Network Type: IN
Owner Address Type: IP4
Owner Address: 192.168.0.160
Session Name (s): SIP Call
Connection Information (c)
Connection Network Type: IN
Connection Address Type: IP4
Connection Address: 192.168.0.160
Time Description, active time (t)
Session Start Time: 0
Session Stop Time: 0
Media Description, name and address (m)
Media Type: audio
Media Port: 5004

```
      Media Proto: RTP/AVP
      Media Format: 4
      Media Format: 2
      Media Format: 15
   Media Attribute (a): rtpmap:4 G723/8000
      Media Attribute Fieldname: rtpmap
      Media Attribute Value: 4 G723/8000
   Media Attribute (a): rtpmap:2 G726-32/8000
   Media Attribute (a): rtpmap:15 G728/8000
   Media Attribute (a): ptime:960
```

- Respuesta del SIP Proxy indicando que esta tratando de localizar al usuario "*3306478*" a través del código de respuesta *100 trying.*

```
Internet Protocol
     Source: 192.168.0.1 (192.168.0.1)
     Destination: 192.168.0.160 (192.168.0.160)
Session Initiation Protocol
     Status-Line: SIP/2.0 100
        Status-Code: 100
        Resent Packet: False
     Message Header … (igual al anterior pero sin el SDP)
```

- Invitación del SIP Proxy al usuario "*3306478*". Este recibe toda la descripción de la sesión a la cual esta siendo invitado por medio del Protocolo de Descripción de Sesión *SDP*.

Internet Protocol

Source: 192.168.0.1 (192.168.0.1)

Destination: 192.168.0.161 (192.168.0.161)

Session Initiation Protocol

Request-Line: ***INVITE***

sip:3306478@192.168.0.161;user=phone SIP/2.0

Message Header

Record-Route:

<sip:3306478@192.168.0.1;ftag=18b85c51d64ea7ef;lr=on>

Via: SIP/2.0/UDP

192.168.0.1;branch=z9hG4bK9bec.00c64274.0

Via: SIP/2.0/UDP

192.168.0.160;branch=z9hG4bK506b1fd57eadbfc6

From:

SIP from address: "Andres Parra"

<sip:***3304076***@prosip.com;user=phone>

SIP tag: 18b85c51d64ea7ef

To: <sip:***3306478***@prosip.com;user=phone>

Contact: <sip:3304076@192.168.0.160;user=phone>

Call-ID: 7818bc8158c868ad@192.168.0.160

CSeq: 12775 ***INVITE***

User-Agent: Grandstream HT286 1.0.4.49

Max-Forwards: 69

Content-Type: ***application/sdp***

Content-Length: 202

Message body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator

Owner Username: 3304076

Session ID: 8000

Session Version: 8000

Owner Network Type: IN

Owner Address Type: IP4
Owner Address: 192.168.0.160
Session Name (s): SIP Call
Connection Information (c): IN IP4
192.168.0.160
Time Description, active time (t): 0 0
Media Description, name and address (m):
audio 5004 RTP/AVP 4 2 15
Media Attribute (a): rtpmap:4 G723/8000
Media Attribute (a): rtpmap:2 G726-32/8000
Media Attribute (a): rtpmap:15 G728/8000
Media Attribute (a): ptime:960

- Respuesta del usuario "*3306478*" indicando que esta tratando de localizar al usuario "*3304076*" a través el código *100 trying.*

Internet Protocol
Source: 192.168.0.161 (192.168.0.161)
Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
Status-Line: SIP/2.0 100 trying
Status-Code: 100
Resent Packet: False
Message Header
Via: SIP/2.0/UDP
192.168.0.1;branch=z9hG4bK9bec.00c64274.0
Via: SIP/2.0/UDP
192.168.0.160;branch=z9hG4bK506b1fd57eadbfc6
From:
SIP from address: "Andres Parra"
<sip:3304076@prosip.com;user=phone>

```
            SIP tag: 18b85c51d64ea7ef
         To: <sip:3306478@prosip.com;user=phone>
         Call-ID: 7818bc8158c868ad@192.168.0.160
         CSeq: 12775 INVITE
         User-Agent: Grandstream HT286 1.0.4.50
         Content-Length: 0
```

- El usuario "*3306478*" envía el código *180 Ringing* indicando que esta timbrando.

```
Internet Protocol
      Source: 192.168.0.161 (192.168.0.161)
      Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
      Status-Line: SIP/2.0 180 ringing
         Status-Code: 180
         Resent Packet: False
      Message Header
         Via: SIP/2.0/UDP
         192.168.0.1;branch=z9hG4bK9bec.00c64274.0
         Via: SIP/2.0/UDP
         192.168.0.160;branch=z9hG4bK506b1fd57eadbfc6
         Record-Route:
         <sip:3306478@192.168.0.1;ftag=18b85c51d64ea7ef;lr=on>
         From:
               SIP from address: "Andres Parra"
               <sip:3304076@prosip.com;user=phone>
               SIP tag: 18b85c51d64ea7ef
         To: <sip:3306478@prosip.com;user=phone>;
            tag=5352d1061475e80e
```

```
Call-ID: 7818bc8158c868ad@192.168.0.160
CSeq: 12775 INVITE
User-Agent: Grandstream HT286 1.0.4.50
Content-Length: 0
```

- El SIP Proxy envía el mismo código *180 Ringing* al usuario que inicia la llamada "*3304076*" para que este escuche el timbre en la bocina.

```
Internet Protocol
     Source: 192.168.0.1 (192.168.0.1)
     Destination: 192.168.0.160 (192.168.0.160)
Session Initiation Protocol
     Status-Line: SIP/2.0 180 ringing
        Status-Code: 180
        Resent Packet: False
     Message Header
        Via: SIP/2.0/UDP
        192.168.0.160;branch=z9hG4bK506b1fd57eadbfc6
        Record-Route:
        <sip:3306478@192.168.0.1;ftag=18b85c51d64ea7ef;lr=on>
        From:
             SIP from address: "Andres Parra"
             <sip:3304076@prosip.com;user=phone>
             SIP tag: 18b85c51d64ea7ef
        To: <sip:3306478@prosip.com;user=phone>;
           tag=5352d1061475e80e
        Call-ID: 7818bc8158c868ad@192.168.0.160
        CSeq: 12775 INVITE
        User-Agent: Grandstream HT286 1.0.4.50
        Content-Length: 0
```

- El usuario “*3306478*” contesta el teléfono y de esta manera acepta la invitación. Entonces el Ata 2 envía un comando *200 OK* indicando al SIP Proxy que se levanto la bocina y todo se ha hecho satisfactoriamente. Además envía todos sus datos a través del SDP.

```
Internet Protocol
     Source: 192.168.0.161 (192.168.0.161)
     Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
     Status-Line: SIP/2.0 200 OK
        Status-Code: 200
        Resent Packet: False
     Message Header
        Via: SIP/2.0/UDP
        192.168.0.1;branch=z9hG4bK9bec.00c64274.0
        Via: SIP/2.0/UDP
        192.168.0.160;branch=z9hG4bK506b1fd57eadbfc6
        Record-Route:
        <sip:3306478@192.168.0.1;ftag=18b85c51d64ea7ef;lr=on>
        From:
             SIP from address: "Andres Parra"
             <sip:3304076@prosip.com;user=phone>
             SIP tag: 18b85c51d64ea7ef
        To: <sip:3306478@prosip.com;user=phone>;
             tag=5352d1061475e80e
        Call-ID: 7818bc8158c868ad@192.168.0.160
        CSeq: 12775 INVITE
        User-Agent: Grandstream HT286 1.0.4.50
        Contact: <sip:3306478@192.168.0.161;user=phone>
        Content-Type: application/sdp
        Content-Length: 148
     Message body
```

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o):

3306478 8000 8000 IN IP4 192.168.0.161

Session Name (s): SIP Call

Connection Information (c): IN IP4

192.168.0.161

Time Description, active time (t): 0 0

Media Description, name and address (m):

audio 5004 RTP/AVP 4

Media Attribute (a): rtpmap:4 G723/8000

Media Attribute (a): ptime:30

- Inmediatamente el SIP Proxy envía la respuesta *200 OK* al usuario que inicia la llamada "*3304076*" indicándole que el usuario destino ha atendido la llamada y que todo se ha hecho satisfactoriamente. Además reenvía la Descripción de la sesión tal cual como la recibió.

Internet Protocol

Source: 192.168.0.1 (192.168.0.1)

Destination: 192.168.0.160 (192.168.0.160)

Session Initiation Protocol

Status-Line: SIP/2.0 200 OK

Status-Code: 200

Resent Packet: False

Message Header …

Message body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o):

3306478 8000 8000 IN IP4 192.168.0.161

Session Name (s): SIP Call
Connection Information (c): IN IP4
192.168.0.161
Time Description, active time (t): 0 0
Media Description, name and address (m):
audio 5004 RTP/AVP 4
Media Attribute (a): rtpmap:4 G723/8000
Media Attribute (a): ptime:30

- El Usuario llamado “3306478” envía al SIP Proxy el comando final de respuesta *ACK* para iniciar la conversación.

Internet Protocol
Source: 192.168.0.160 (192.168.0.160)
Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
Request-Line: ACK sip:3306478@192.168.0.161;user=phone SIP/2.0
Method: ACK
Resent Packet: False
Message Header …
CSeq: 12775 ***ACK***
User-Agent: Grandstream HT286 1.0.4.49
Max-Forwards: 70
Content-Length: 0

- El SIP Proxy reenvía al usuario que inicia la llamada “3304076” el mismo *Comando Final de respuesta ACK.* De aquí en adelante la comunicación

ya esta establecida y durara hasta que uno de los dos usuarios termine la llamada.

```
Internet Protocol
      Source: 192.168.0.1 (192.168.0.1)
      Destination: 192.168.0.161 (192.168.0.161)
Session Initiation Protocol
      Request-Line: ACK sip:3306478@192.168.0.161;user=phone
      SIP/2.0
      Message Header …
         CSeq: 12775 ACK
         User-Agent: Grandstream HT286 1.0.4.49
         Max-Forwards: 69
         Content-Length: 0
```

- Finalmente, el usuario "*3304076*" cuelga el teléfono y da por finalizada la llamada. El Ata 1 envía entonces un comando *BYE* al SIP Proxy para indicar el fin de la llamada.

```
Internet Protocol
      Source: 192.168.0.161 (192.168.0.161)
      Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
      Request-Line: BYE sip:3304076@192.168.0.160;user=phone
      SIP/2.0
         Method: BYE
         Resent Packet: False
      Message Header ..
         CSeq: 32145 BYE
```

User-Agent: Grandstream HT286 1.0.4.50
Max-Forwards: 70
Content-Length: 0

- Inmediatamente el SIP Proxy reenvía al usuario "*3306478*" el mismo comando *BYE* para indicarle que la llamada ha sido finalizada.

Internet Protocol
Source: 192.168.0.1 (192.168.0.1)
Destination: 192.168.0.160 (192.168.0.160)
Session Initiation Protocol
Request-Line: BYE sip:3304076@192.168.0.160;user=phone SIP/2.0
Method: BYE
Resent Packet: False
Message Header …
CSeq: 32145 ***BYE***
User-Agent: Grandstream HT286 1.0.4.50
Max-Forwards: 69
Content-Length: 0

- El usuario "*3306478*" responde al SIP Proxy con un código ***200 OK*** para indicar que recibió las instrucciones y que todo se hizo satisfactoriamente.

Internet Protocol
Source: 192.168.0.160 (192.168.0.160)
Destination: 192.168.0.1 (192.168.0.1)

Session Initiation Protocol

Status-Line: SIP/2.0 200 OK

Status-Code: 200

Resent Packet: False

Message Header …

CSeq: 32145 ***BYE***

User-Agent: Grandstream HT286 1.0.4.49

Contact: <sip:3304076@192.168.0.160;user=phone>

Content-Length: 0

- Inmediatamente el SIP Proxy reenvía el mismo código de estado *200 OK* al usuario "*3304076*" para indicarle que el usuario "*3306478*" recibió el fin de la llamada exitosamente.

Internet Protocol

Source: 192.168.0.1 (192.168.0.1)

Destination: 192.168.0.161 (192.168.0.161)

Session Initiation Protocol

Status-Line: SIP/2.0 200 OK

Status-Code: 200

Resent Packet: False

Message Header …

CSeq: 32145 ***BYE***

User-Agent: Grandstream HT286 1.0.4.49

Contact: <sip:3304076@192.168.0.160;user=phone>

Content-Length: 0

- **Situación 6. El usuario al cual se desea localizar no existe o no se encuentra registrado**.

En este caso los usuarios “3304076” y “3306478” se encuentran registrados correctamente. El Usuario “3304076” con el Ata 1 hace una llamada a un tercer usuario “3306475” el cual no se encuentra registrado en el SIP Proxy Server. Solo se pueden establecer llamadas entre los usuarios que hallan sido registrados en la base de datos *“Location*” del SER. De lo contrario se observara una situación como la siguiente.

- Invitación del Usuario *“3304076”* al Usuario *“3306475”*.

```
Ethernet II
     Destination: 00:0b:6a:39:9d:9c (192.168.0.1)
     Source: 00:0b:82:00:79:2f (192.168.0.160)
Internet Protocol
     Source: 192.168.0.160 (192.168.0.160)
     Destination: 192.168.0.1 (192.168.0.1)
User Datagram Protocol
     Source port: 5060 (5060)
     Destination port: 5060 (5060)
Session Initiation Protocol
     Request-Line: INVITE sip:3304075@prosip.com;user=phone
     SIP/2.0
        Method: INVITE
        Resent Packet: False
     Message Header
        Via: SIP/2.0/UDP
        192.168.0.160;branch=z9hG4bK55dbeb26151f4597
        From:
             SIP from address: "Andres Parra"
             <sip:3304076@prosip.com;user=phone> (*2)
             SIP tag: a4edf4046c829c1a
```

```
      To: <sip:3304075@prosip.com;user=phone> (*3)
      Contact: <sip:3304076@192.168.0.160;user=phone>
      Call-ID: c0c833f9befa65de@192.168.0.160
      CSeq: 28602 INVITE
      User-Agent: Grandstream HT286 1.0.4.49
      Max-Forwards: 70
      Content-Type: application/sdp
      Content-Length: 202
   Message body
      Session Description Protocol
         Session Description Protocol Version (v): 0
         Owner/Creator, Session Id (o):
            3304076 8000 8000 IN IP4 192.168.0.160
         Session Name (s): SIP Call
         Connection Information (c): IN IP4
         192.168.0.160
         Time Description, active time (t): 0 0
         Media Description, name and address (m):
            audio 5004 RTP/AVP 4 2 15
         Media Attribute (a): rtpmap:4 G723/8000
         Media Attribute (a): rtpmap:2 G726-32/8000
         Media Attribute (a): rtpmap:15 G728/8000
         Media Attribute (a): ptime:960
```

- El SIP Proxy Server retorna el código *404 Not Found* para indicar al que inicia la llamada "*3304076*" que no existe el usuario "*3304075*".

```
Ethernet II
      Destination: 00:0b:82:00:79:2f (192.168.0.160)
      Source: 00:0b:6a:39:9d:9c (192.168.0.1)
Internet Protocol
```

Source: 192.168.0.1 (192.168.0.1)

Destination: 192.168.0.160 (192.168.0.160)

Session Initiation Protocol

Status-Line: SIP/2.0 404 Not Found

Status-Code: 404

Resent Packet: False

Message Header …

CSeq: 28602 ***INVITE***

Server: Sip EXpress router (0.8.12 (i386/linux))

Content-Length: 0

- Finalmente el usuario que inicia la llamada "*3304076*" envía un comando ***ACK*** al SIP **Proxy** para indicarle que recibió la notificación de usuario no encontrado.

Ethernet II

Destination: 00:0b:6a:39:9d:9c (192.168.0.1)

Source: 00:0b:82:00:79:2f (192.168.0.160)

Internet Protocol

Source: 192.168.0.160 (192.168.0.160)

Destination: 192.168.0.1 (192.168.0.1)

Session Initiation Protocol

Request-Line: ACK sip:3304075@prosip.com;user=phone SIP/2.0

Method: ACK

Resent Packet: False

Message Header …

CSeq: 28602 ***ACK***

User-Agent: Grandstream HT286 1.0.4.49

Max-Forwards: 70

Content-Length: 0

❖ **Situación 7. La línea del usuario llamado se encuentra ocupada**.

Para este caso se levanta la bocina del usuario “3304076” con el Ata 1 para simular que la línea está ocupada. De esta manera el intento del usuario que inicia la llamada “3306478” con el Ata 2 para establecer una llamada no es posible mientras el usuario al que está llamando no tenga configurada la opción de llamada en espera (como en este caso).

Se parte de la respuesta del usuario “3304076” al SIP Proxy ya que los primeros pasos de invitación con el comando *INVITE* se han explicado e ilustrado anteriormente.

➢ El usuario llamado “*3304076*” retorna un código *100 Trying* al SIP Proxy indicando que esta intentando establecer comunicación.

```
Ethernet II
     Destination: 00:0b:6a:39:9d:9c (192.168.0.1)
     Source: 00:0b:82:00:79:2f (192.168.0.160)
Internet Protocol
     Source: 192.168.0.160 (192.168.0.160)
     Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
     Status-Line: SIP/2.0 100 trying
        Status-Code: 100
        Resent Packet: False
     Message Header …
        CSeq: 34447 INVITE
        User-Agent: Grandstream HT286 1.0.4.49
        Content-Length: 0
```

- Inmediatamente se da cuenta de que la línea esta ocupada envía un comando *486 Busy* al SIP Proxy para indicar esta situación.

```
Ethernet II,
      Destination: 00:0b:6a:39:9d:9c (192.168.0.1)
      Source: 00:0b:82:00:79:2f (192.168.0.160)
Internet Protocol
      Source: 192.168.0.160 (192.168.0.160)
      Destination: 192.168.0.1 (192.168.0.1)
Session Initiation Protocol
      Status-Line: SIP/2.0 486 busy
         Status-Code: 486
         Resent Packet: False
      Message Header …
         CSeq: 34447 INVITE
         User-Agent: Grandstream HT286 1.0.4.49
         Content-Length: 0
```

- El SIP Proxy retorna al usuario ocupado un comando de respuesta final *ACK* indicándole que recibió la información y que la comunicación no se establecerá.

```
Ethernet II
      Destination: 00:0b:82:00:79:2f (192.168.0.160)
      Source: 00:0b:6a:39:9d:9c (192.168.0.1)
Internet Protocol
      Source: 192.168.0.1 (192.168.0.1)
      Destination: 192.168.0.160 (192.168.0.160)
Session Initiation Protocol
```

Request-Line: ACK sip:3304076@192.168.0.160;user=phone SIP/2.0

Method: ACK

Resent Packet: False

Message Header …

CSeq: 34447 ***ACK***

User-Agent: Sip EXpress router(0.8.12 (i386/linux))

Content-Length: 0

- Inmediatamente después el SIP Proxy envía al usuario que inicia la llamada "*3306478*" un código de estado *486 Busy* indicándole que el usuario llamado se encuentra ocupado y no puede establecer una conversación con este.

Ethernet II

Destination: 00:0b:82:00:79:26 (192.168.0.161)

Source: 00:0b:6a:39:9d:9c (192.168.0.1)

Internet Protocol

Source: 192.168.0.1 (192.168.0.1)

Destination: 192.168.0.161 (192.168.0.161)

Session Initiation Protocol

Status-Line: SIP/2.0 486 busy

Status-Code: 486

Resent Packet: False

Message Header …

CSeq: 34447 INVITE

User-Agent: Grandstream HT286 1.0.4.49

Content-Length: 0

- Finalmente el usuario que inicia la llamada "*3306478*" retorna al SIP **Proxy** un comando de respuesta final ***ACK*** indicándole que recibió

satisfactoriamente la información.

Ethernet II

Destination: 00:0b:6a:39:9d:9c (192.168.0.1)

Source: 00:0b:82:00:79:26 (192.168.0.161)

Internet Protocol

Source: 192.168.0.161 (192.168.0.161)

Destination: 192.168.0.1 (192.168.0.1)

Session Initiation Protocol

Request-Line: ACK sip:3304076@prosip.com;user=phone SIP/2.0

Method: ACK

Resent Packet: False

Message Header …

CSeq: 34447 ***ACK***

User-Agent: Grandstream HT286 1.0.4.50

Max-Forwards: 70

Content-Length: 0

8. CONCLUSIONES

El desarrollo y la implementación de un servicio de VoIP no tiene gran costo económico como se pudo ver a lo largo del trabajo; en cambio si tiene un alto costo intelectual, pues son una gran cantidad de conceptos y procesos los que se tienen que fundir para obtener la herramienta mas importante y esencial en este proyecto: el conocimiento. Una vez se tiene el conocimiento requerido solo es cuestión de organizar ideas y plasmarlas a la hora de la implementación, configuración, depuración y ejecución de cada uno de los sistemas necesarios para formar el Servicio de Telefonía IP.

El obstáculo que representa el mayor impedimento para que este proyecto sea de gran utilidad para la sociedad, es desafortunadamente la regulación de las telecomunicaciones vigente en Colombia y muchas otras partes del mundo. Con toda razón hay muchos intereses y dinero de por medio que han invertido las compañías operadoras de larga distancia nacional e internacional, pues hace varios años pagaron por unos derechos que deben ser respetados, pues representaron una gran inversión en tiempo y en dinero; sin embargo, para infortunio de todos, no se hicieron en un momento en el cual la tecnología tuviera a su disposición una opción tan robusta y económica como esta. Queda entonces esperar unos pocos años para prestar este servicio a toda la comunidad estando ya cobijada esta variación por la ley.

En este momento se pueden ofrecer todas las ventajas de la Telefonía IP a las empresas que cuentan con sucursales en varias ciudades o países, y en las que el gasto por marcación telefónica a larga distancia es bastante representativo.

La inversión inicial no es muy alta y depende mucho de las necesidades del cliente, pues como se expreso en el documento existen varias alternativas de Ínterconectividad que varían en funcionalidad y costo. Son necesarios unos gastos de manteniendo y soporte técnico que fácilmente pueden cubrir la mayor parte de las compañías en Colombia.

Por otro lado, se le ofrece este servicio a las compañías prestadoras de los servicios de Internet de Banda Ancha (ADSL, Cable MODEM actualmente) para que lo presenten a sus usuarios como un contenido que hace mucho mas atractivo y funcional su enlace de alta velocidad.

El desarrollo e implementación de esta tecnología se concentra principalmente en la generación de aplicaciones de software y en la creatividad de individuos que no pertenezcan exclusivamente a empresas de prestación de servicios. Esto significa que esta tecnología en su núcleo, favorece a la descentralización de los poderes en cuanto a la prestación de servicios de telecomunicaciones y más específicamente a la de prestación de servicios de telefonía pública.

La gran ventaja que se observó en cuanto a la utilización del protocolo SIP es la baja cantidad de flujo de datos necesario para establecer una sesión. Esto es una gran ventaja ya que un servidor configurado como enrutador SIP, posee una alta capacidad de procesamiento y conmutación de llamadas haciéndolo bastante eficiente para un flujo alto de llamadas; esto se traduce en un ahorro considerable en costos de equipos a la hora de implementar un servicio de conmutación de llamadas telefónicas sobre el protocolo de Internet.

Este proyecto es un importante punto de referencia para que se logre un desarrollo continuado por parte de la comunidad universitaria. La posibilidad de generar grupos de investigación y de desarrollo en sistemas de VoIP está a la mano ya que se cuenta con los recursos de infraestructura por parte de las universidades de Colombia y por supuesto con la masiva cantidad de información que poseen, generan y comparten grupos de investigación y desarrollo en todo el mundo.

Se proyecta que en un periodo de 5 años este sistema que sigue en un desarrollo día a día este operando y ofreciendo servicios a empresas colombianas, latinoamericanas y algunas multinacionales en Sur y Centro América. Otro escenario proyectado es el desarrollo en conjunto con empresas prestadoras de servicios de telefonía tanto local como larga distancia como EMCALI, TELECOM y EPM, de una plataforma multi-tecnológica que integre todos los servicios de telecomunicaciones, agregando algunos otros (Audio, video, Telefonía, Radio, Internet, etc), en un solo producto, logrando un portafolio de contenidos y servicios muy atractivo dándole un valor agregado a la estructura actual de telecomunicaciones.

Finalmente, la gran ventaja de la implementación de servicios de telefonía IP mediante el protocolo SIP es el alto grado de flexibilidad, lo cual será un factor clave para estimular la competencia y por ende la mejora de los servicios de telefonía prestados al público.

BIBLIOGRAFÍA

Cisco ATA 186 [en línea]. Stanford : Cisco Systems, 2003. [Citado 11 de feb, 2004]. Disponible por internet : www.cisco.com/warp/public/cc/pd/as/180/186.

HandyTone User Manual [en línea]. Chicago : Grandstream Networks inc, 2002. [Citado 11 de feb, 2004]. Disponible por internet : http://www.grandstream.com/user_manuals/HandyTone.

Internet Web Server and Domain Configuration Tutorial [en línea]. New York : Greg Ippolito, 2003. [Citado 5 de mar, 2004]. Disponible por internet : http://www.yolinux.com/ TUTORIALSLinuxTutorialWebSiteConfig.html.

La telefonía sobre IP [en línea]. Madrid : José Manuel Huidobro, 2003. [Citado 5 de abr, 2004]. Disponible por internet : http://www.monografias.com/trabajos10/tele/tele.shtml.

MAXWELL, Steve. Red Hat Linux : Herramientas para la administración de redes. Bogotá : McGraw-Hill, 2001. 715p. + 2 Discos Compactos. ISBN 958-41-0220-6.

MySQL Reference Manual [en línea]. Seattle : MYSQL AB, 2003. [Citado 5 de mar, 2004]. Disponible por internet : http://dev.mysql. com/doc.

NAT and Firewall Scenarios and Solutions for SIP [en línea]. East Hanover : IETF, 2002. [Citado 5 de abr, 2004]. Disponible por internet : http://www.ietf.org/internet-drafts/draft-ietf-sipping-nat-scenarios-00.txt.

Php Manual [en línea]. Chicago : Php Group, 2003. [Citado 5 de mar, 2004]. Disponible por internet : http://www.php.net/ manual/en.

SDP : Session Description Protocol [en línea]. Cambridge : Network Working Group, 1998. [Citado 5 de abr, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc2327.txt.

SIP Cookbook : SER Configuration [en línea]. Boston : Jeremy George, 2003. [Citado 25 de feb, 2004]. Disponible por internet : http://www.mit.edu/afs/athena/project/sip/sip.edu/ser.shtml.

SIP Express Router [en línea]. Berlin : Iptel, 2003. [Citado 04 de feb, 2004]. Disponible por internet : www.iptel.org/ser.

SIP : Session Initiation Protocol [en línea]. East Hanover : Network Working Group, 2002. [Citado 1 de feb 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3261.txt.

Solving the Firewall and NAT Traversal Issues for Multimedia Over IP Services [en línea]. Ottawa : Newport Networks System Coporation, 2004. [Citado 10 de may 2004]. Disponible por internet : http://www.newport-networks.com/FW-NAT-Trav-WP.pdf.

Symmetric NAT Traversal using STUN [en línea]. San Diego : IETF, 2003. [Citado 5 de abr, 2004]. Disponible por internet : http://www.ietf.org/internet-drafts/draft-takeda-symmetric-nat-traversal-00.txt.

Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [en línea]. Redmond : Network Working Group, 2003. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc3605.txt.

RTP : A Transport Protocol for Real-Time Applications [en línea]. Berlin : Network Working Group, 1996. [Citado 15 de feb, 2004]. Disponible por internet : http://www.ietf.org/rfc/rfc1889.txt.

The Conceptual Architecture of the Apache Web Server [en línea]. Waterloo, 1999. [Citado 8 de mar, 2004]. Disponible por internet : http://www.math.uwaterloo.ca/~oadragoi/CS746G/a1/apache_conceptual_arch.html.

Voice Over IP [en línea]. New York : Prorocols.com Group, 2003. [Citado 05 de feb, 2004]. Disponible por internet : www.protocols.com/pbook/ VoIPFamily.htm.

ZIGLER, Robert. Firewalls Linux : Guía Avanzada. Madrid : Prentice-Hall, 2000. 474p. ISBN 0-7357-0900-9.

ÍNDICE